NETGEAR

Mobile Broadband 11n Wireless Router MBR1210

User Guide

ENGLISH

Routeur sans fil MBR1210 11n à haut débit mobile

Guide d'utilisation

FRANÇAIS



350 East Plumeria Drive
San Jose, CA 95134
USA

October 2010
202-10734-03
v1.0

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at *http://support.netgear.com*.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): See Support information card.

Trademarks

NETGEAR, the NETGEAR logo, ReadyNAS, ProSafe, Smart Wizard, Auto Uplink, X-RAID2, and NeoTV are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT, and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10734-03	v1.0	October 2010	First publication

Table of Contents

Chapter 5 Advanced

Chapter 6 Troubleshooting

Connecting to the Internet

1

This chapter describes how to configure your Routeur sans fil MBR1210 11n à haut débit mobile Internet connection.

- **Hardware Features**
- **Log In to Your Router**
- **Access the Configuration Assistant after Installation**
- **Manually Configure Your Internet Settings**

Note: For help with installation, see the *Mobile Broadband 11n Wireless Router MBR1210 Installation Guide.*

Hardware Features

This section outlines the physical aspects of your Mobile Broadband 11n Wireless Router.

Router Stand

Since the Mobile Broadband 11n Wireless Router is a vertical-only device, use the stand to position your router upright.

1. Insert the tabs on the stand into the slot on the bottom of your router.
2. Place your router near an AC power outlet in a location where you can connect the cables you need for your home network.

   The router must also be located where you can receive a strong mobile broadband signal while indoors if you are planning to connect to the Internet using mobile broadband.

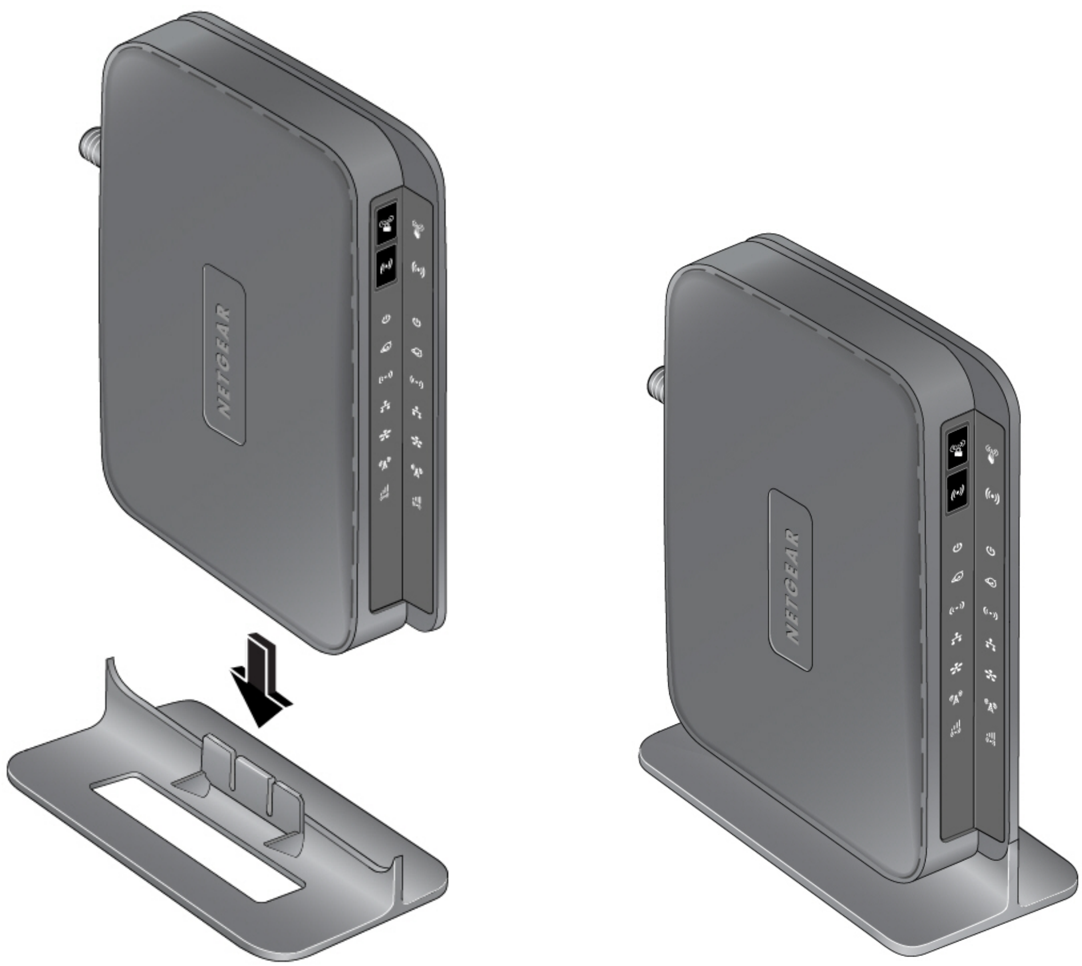


Figure 1.

Router Front Panel

The router front panel contains control buttons and status LEDs. Use the LEDs to verify status and connections.

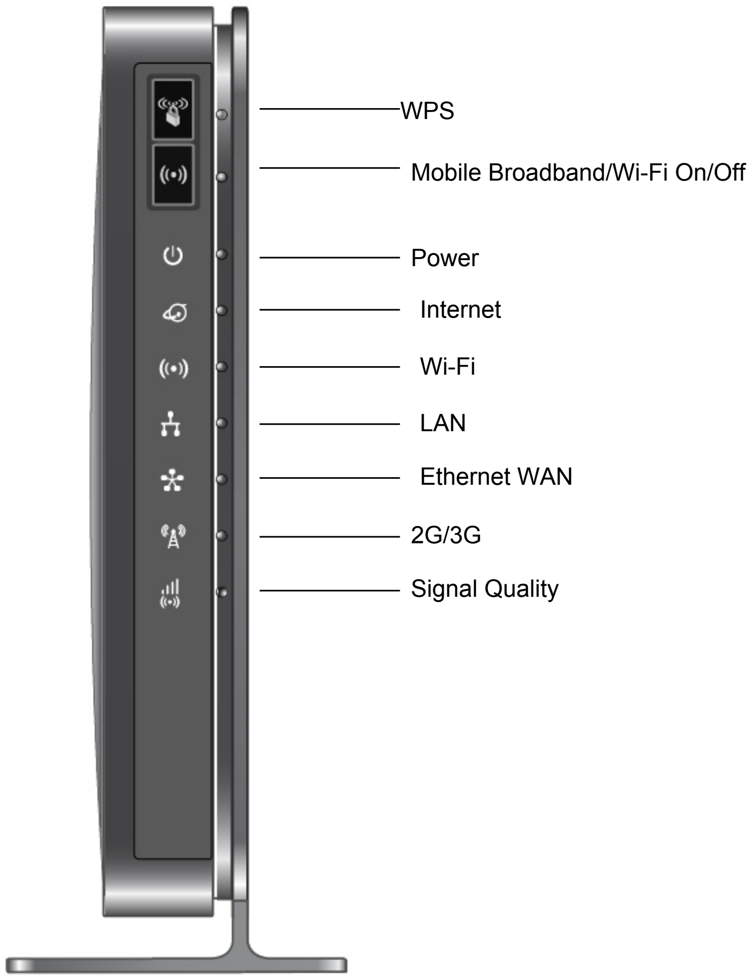


Figure 2.

Table 1 describes each LED and button located on the front panel of the router.

Table 1. LED Descriptions

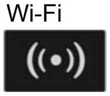
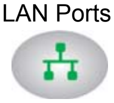
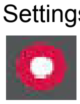
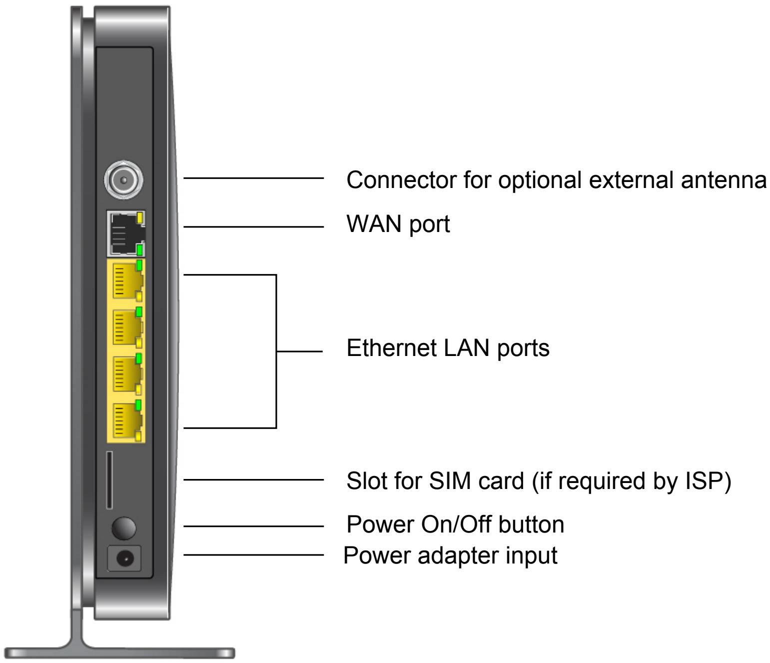
LED	Activity	Description
WPS 	Press the WPS button to open a 2-minute window for the router to connect with other WPS-enabled devices. For more information about this function, see *Use Push 'N' Connect (WPS) to Configure Your Wireless Network* on page 32.	
Wi-Fi 	This button can be used to control the WiFi radio or both the WiFi radio and mobile broadband radio. Use the router interface to select the options. The default is set for Wi-Fi radio only.	

Table 1. LED Descriptions

LED	Activity	Description
Power 	Solid green	The router is turned on and operating normally.
	Solid amber	POST (power-on self-test) in progress.
	Off	Power is not supplied to the router.
Internet Port 	Solid green	There is an Internet session.
	Solid amber	Traffic meter limit has been reached, traffic is blocked.
	Blinking green	Data is being transmitted over the Internet connection.
	Blinking amber	Traffic meter limit has been reached, but traffic not blocked.
	Blinking green and amber	Failover from WAN to Mobile Broadband.
	Off	No Internet connection detected.
Wi-Fi 	Solid blue	The Wi-Fi local port is initialized.
	Blinking blue	Data is being transmitted or received over the Wi-Fi link.
	Off	The wireless access point is turned off.
LAN Ports 	Solid green	The local Ethernet ports have detected wired links with PCs.
	Blinking	Data is being transmitted or received.
	Off	No link is detected on these ports.
WAN Port 	Solid green	The Ethernet WAN port has detected an active link.
	Blinking	Data is being transmitted or received.
	Off	No link is detected on these ports.
2G/3G 	Solid blue	Indicates the router is in 3G+ coverage.
	Solid green	Indicates the router is in 2G coverage.
	Off	No coverage is detected.
Signal Quality 	Solid blue	Excellent coverage detected.
	Solid green	Good coverage detected.
	Solid amber	Marginal coverage detected.
	Off	No coverage detected.
Restore Factory Settings 	Locate the small hole outlined in red on the back of the router. Insert a paperclip into the hole and push for 6 seconds. Depressing the reset button causes the LED to blink briefly. After the button is held down for more than 6 seconds, the LED will flash AMBER, and then turn green as the router resets to the factory defaults. See	

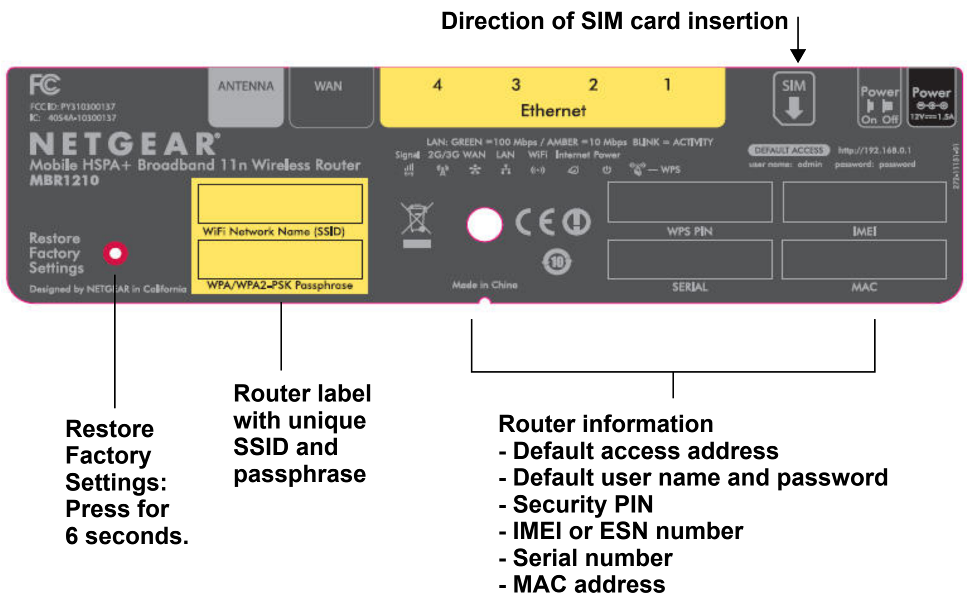
Router Back Panel

The back panel of the router contains port connections.



Router Label

The label on the left side of the router shows the router's MAC address, serial number, security PIN, IMEI or ESN number, and factory default login information. It also contains the SSID and passphrase that is unique to each router.



Log In to Your Router

When you first connect to your router during installation, a Setup Wizard displays. For help using the Setup Wizard to configure your Internet and wireless network, see the *Mobile Broadband 11n Wireless Router MBR1210 Installation Guide*.

After the initial configuration, you can use your Web browser to log in to the router to view or change its settings. Links to Knowledge Base and documentation are also available on the router main menu.

Note: Your computer must be configured for DHCP. For help configuring DHCP, refer to the documentation that came with your computer, or see the link to the online document in *Preparing Your Network* in Appendix A.

When you have logged in, if you do not click **Logout**, after 5 minutes of no activity the router automatically logs you out.

To log in to the router:

1. Type **http://www.routerlogin.net** in the address field of your browser, and then press enter to display the login window.



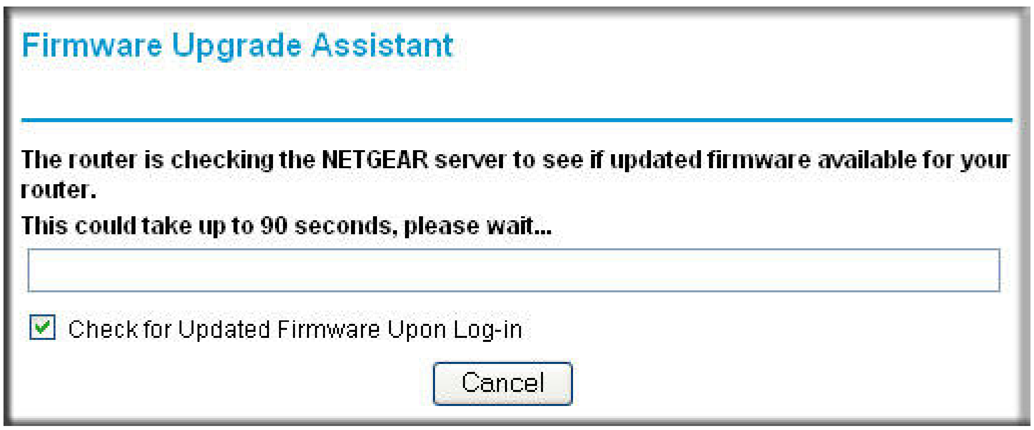
2. Enter **admin** for the user name and your password (or the default, **password**).

   For information about how to change the password, see *Changing the Built-In Password* on page 55.

Note: If you do not remember your password, you can restore the router to its factory default settings, which will reset the password. See *Factory Default Settings* on page 93.

3. If the router has not been configured, the Smart Wizard screen displays. After the router has been configured, one of the following screens appears:
    - **Firmware Upgrade Assistant screen**. After initial setup, the Firmware Upgrade Assistant screen displays unless the **Check for Updated Firmware Upon Log-in** check box is cleared.

Note: You can disable this automatic checking and updating feature during future log ins by clearing the **Check for Updated Firmware Upon Log-in** check box, but NETGEAR recommends that you keep this feature enabled to ensure your router is using the latest updated firmware.



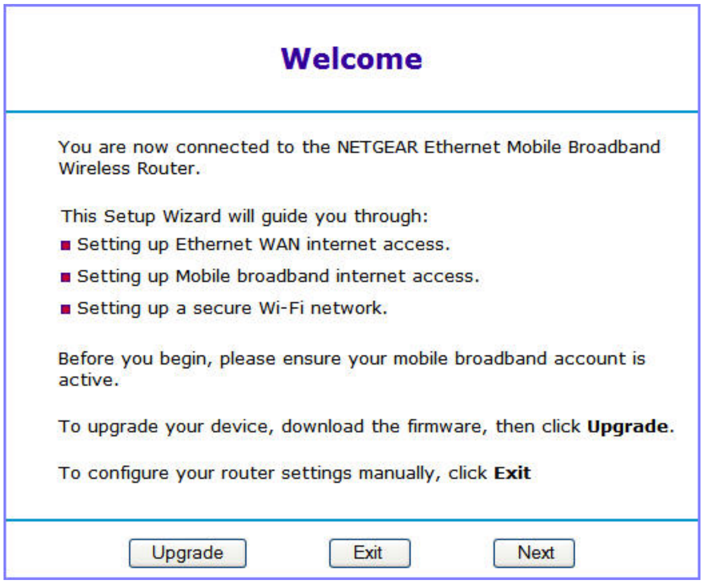
- **Router Status screen**. The Router Status screen displays the current router connection status. See *Router Status* on page 48.

4. You can use different methods to configure your router.
    - Select Setup Wizard **from the router menu to set up your Internet connection and wireless network configuration**. See *Access the Configuration Assistant after Installation* on page 14.
    - You can manually configure the router settings. See *Manually Configure Your Internet Settings* on page 15.

Access the Configuration Assistant after Installation

1. Log in to the router as described in *Log In to Your Router* on page 12.

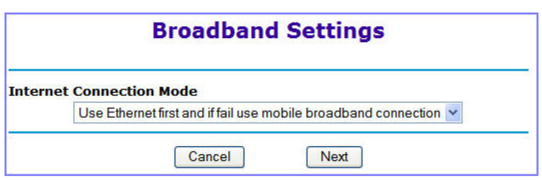
   The Configuration Assistant opens.



2. Click **Next**.

   The Configuration Assistant prompts you to set up your Internet connection and wireless network as described in the *Mobile Broadband 11n Wireless Router MBR1210 Installation Guide*.

   a. Select your Internet connection mode:
      - Use Ethernet first and if fail use mobile broadband connection
      - Always use mobile broadband connection
      - Always use Ethernet connection



   b. Click **Next**.

   c. Select your **country** and then your **Internet Service Provider**.

   d. Click **Done**.

Manually Configure Your Internet Settings

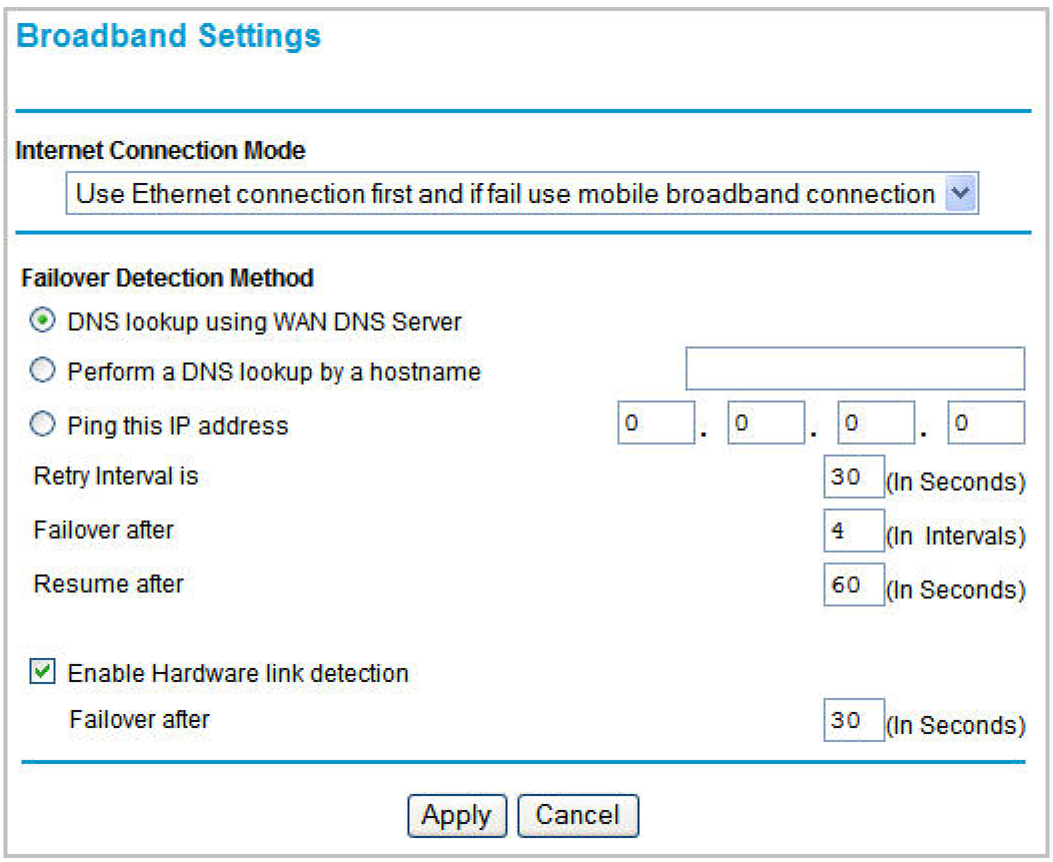
For you to connect to the network, an active broadband service account is required. Contact your ISP for your user name, password, and the network name. You must also configure some or all of the settings described in the following sections, depending on how you have chosen to connect to the Internet:

- *Broadband Settings* on page 15.
- *Mobile Broadband Settings* on page 17 (not required if using Ethernet connection only).
- *Ethernet Broadband Settings* on page 19 (not required if using mobile broadband connection only).

Broadband Settings

To manually configure your broadband Internet settings:

1. Log in to the router as described in *Log In to Your Router* on page 12.
2. From the main menu, select Broadband Settings.



3. Adjust the settings as needed based on your Internet connection. The fields in this screen are described in *Table 2*.
4. The following buttons are available:
   - **Apply**. Apply the changes that you made.
   - **Cancel**. Discard changes.

Table 2. Internet Connection Settings

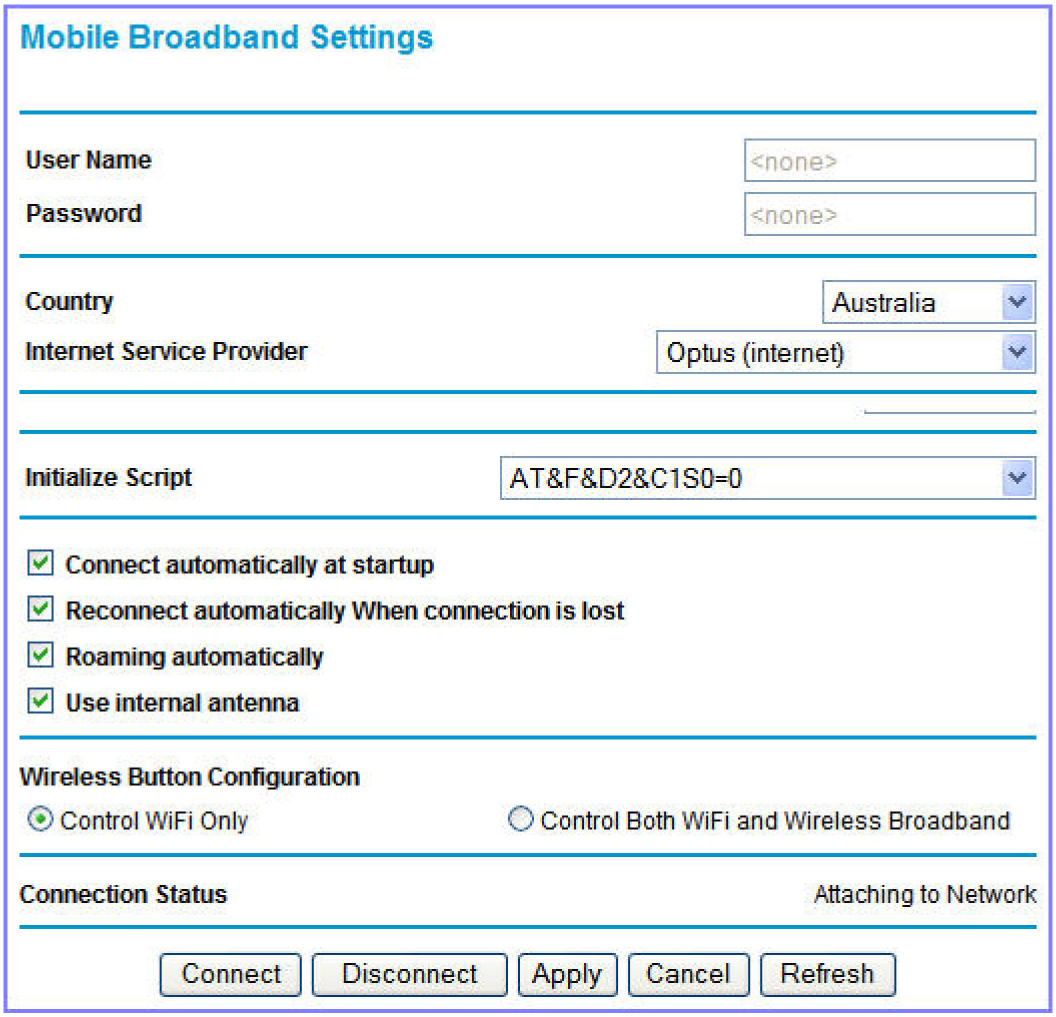
Fields and Check Boxes	Description
Internet Connection Mode	The choices are: • Always use an Ethernet connection (default) • Use Ethernet first and if it fails use mobile broadband connection • Always use mobile broadband connection
Failover Detection Method[1]	Select the failover method and enter the related information: • DNS lookup using WAN DNS Server • Perform a DNS lookup by a hostname • Ping this IP address
Retry Interval is[1]	Enter the retry interval.
Failover after[1]	Enter how many retry attempts to make before failing over.
Resume after[1]	Enter how long to wait for primary link is stabilized before resuming to use the primary link.
Enable Hardware link detection	Enter when to failover when the Ethernet link is dropped. This is independent of the DNS / Ping detection methods.

1 This field is available only when the Internet Connection Mode is ***Use Ethernet first and if fail use 3G mobile connection.***

Mobile Broadband Settings

To manually configure your mobile broadband Internet settings:

1. Log in to the router as described in *Log In to Your Router* on page 12.
2. From the main menu, select Mobile Broadband Settings.



3. Adjust the settings as needed based on your Internet connection. The fields in this screen are described in *Table 3*.
4. Available buttons are:
   - **Connect**. Manually connect to the network.
   - **Disconnect**. Disconnect from the current network.
   - **Apply**. Apply the changes that you made.
   - **Cancel**. Discard changes.
   - **Refresh**. Update the connection status

Table 3. Settings

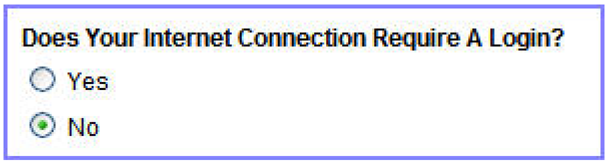
Fields and Check Boxes	Description
User Name	Internet account login user name.
Password	Internet account password for authentication.
Country	Select your country from the drop-down list.
Internet Service Provider	Select your Internet Service Provider from the drop-down list.
Access Number	The remote site's phone number.
PIN code	Pin code of the SIM card, where applicable.
APN	Access point name.
PDP type	Select the type of packet data protocol: • **IP** • **PDP-IP** • **PPP** • **PPP-IP**
Connect automatically at startup	When this check box is selected, the modem automatically connects to the network when powered up. This should be selected after login information is provided.
Reconnect automatically when connection is lost	When this check box is selected, the modem will attempt to reconnect to the network when the connection is lost. Under normal situations, this setting should be selected.
Roaming automatically	When this check box is checked, the unit might roam to any available operator in range and might incur roaming charges.
Use internal antenna	If this check box is selected, the router will use the internal antenna rather than the external antenna.
Wireless Button Configuration	Select the option to determine the behavior of the WPS push button on the front panel when pressed. • **Control Wi-Fi Only** : Pressing the push button toggles the Wi-Fi function. If Wi-Fi is turned on, pressing the push button turns off the Wi-Fi. Pressing it again will turn on the Wi-Fi. This function is available only if the Wi-Fi function is enabled. The Wireless Broadband function is unaffected. • **Control Both Wi-Fi and Wireless Broadband**: Pressing the push button toggles both the Wi-Fi function and wireless broadband at the same time. If Wi-Fi is turned on, pressing the push button turns off the Wi-Fi. At the same time, the wireless broadband connection is disconnected. If you press the push button again, Wi-Fi is turned on and the router attempts to re-establish the wireless broadband connection. Depending on the coverage, wireless broadband coverage might or might not be connected successfully.
Connection status	Current WAN port status.

Ethernet Broadband Settings

To manually configure your Ethernet Broadband Internet settings:

1. Log in to the router as described in *Log In to Your Router* on page 12.
2. From the main menu, select Ethernet Broadband Settings.

   The following question displays at the top of the screen:



Select the option based on the type of account you have with your ISP.

- If you need to enter login information every time you connect to the Internet, or you have a PPPoE account with your ISP, select **Yes**.
- Otherwise, select **No**.

Then fill out the appropriate screen.

For details, see:

step a, Login required on page 20

or

step b, Login not required on page 22.

Note: If you have installed PPP software such as WinPoET (from Earthlink) or Enternet (from PacBell), then you have PPPoE. Select **Yes**. After selecting **Yes** and configuring your router, you do not need to run the PPP software on your PC to connect to the Internet.

a. Login required

Adjust the settings as needed based on your Internet connection. The fields in this screen are described in *Table 4*.



Table 4. Ethernet Broadband Settings When Login Required

Fields and Checkboxes	Description
Internet Service Provider	Select the service provided by your ISP. • Other (PPPoE) is the most common. • PPTP is used in Austria and other European countries. • Telstra BigPond is for Australia only.
Login	This is usually the name that you use in your email address. For example, if your main mail account is JerAB@ISP.com, then put JerAB in this field. Some ISPs (such as Mindspring, Earthlink, and T-DSL) require that you use your full email address when you log in. If your ISP requires your full email address, then type it in the **Login** field.

Table 4. Ethernet Broadband Settings When Login Required

Fields and Checkboxes	Description
Password	Type the password that you use to log in to your ISP.
Service Name (If Required)	If your ISP provided a service name, enter it here. Otherwise, this can be left blank.
Connection Mode	Set the connection mode to **Dial on Demand**, **Always On**, or **Manually Connect**. • With the default setting, **Dial on Demand**, a PPPoE connection automatically starts when there is outbound traffic to the Internet, and it automatically terminates if the connection is idle based on the value in the Idle Timeout field. • When the connection mode is set to **Always On**, the PPPoE connection automatically starts when the computer boots up, but the connection does not time out. The router will keep trying to bring up the connection if it is disconnected for some reason. • If you select **Manually Connect**, you must go to the Router Status screen and click the **Connect** button to connect to the Internet. The manual connection does not time out, and you have to click the **Disconnect** button on the Router Status screen to disconnect it.
Idle Timeout (In Minutes)	An idle Internet connection will be terminated after this time period. If this value is zero (0), then the router will keep the connection alive by reconnecting immediately whenever the connection is lost.
Internet IP Address	If you log in to your service or your ISP did not provide you with a fixed IP address, the router finds an IP address for you automatically when you connect. Select **Get Dynamically from ISP**. If you have a fixed (static, permanent) IP address, your ISP has provided you with an IP address. Select **Use Static IP Address** and type in the IP address.
Domain Name Server (DNS) Address	The DNS server is used to look up site addresses based on their names. • If your ISP gave you one or two DNS addresses, select **Use These DNS Servers** and type the primary and secondary addresses. • Otherwise, select **Get Automatically From ISP**. **Note**: If you get "Address not found" errors when you go to a website, it is likely that your DNS servers are not set up correctly. You should contact your ISP to get DNS server addresses.

b. Login not required

Adjust the settings as needed based on your Internet connection. The fields in this screen are described in *Table 5*.

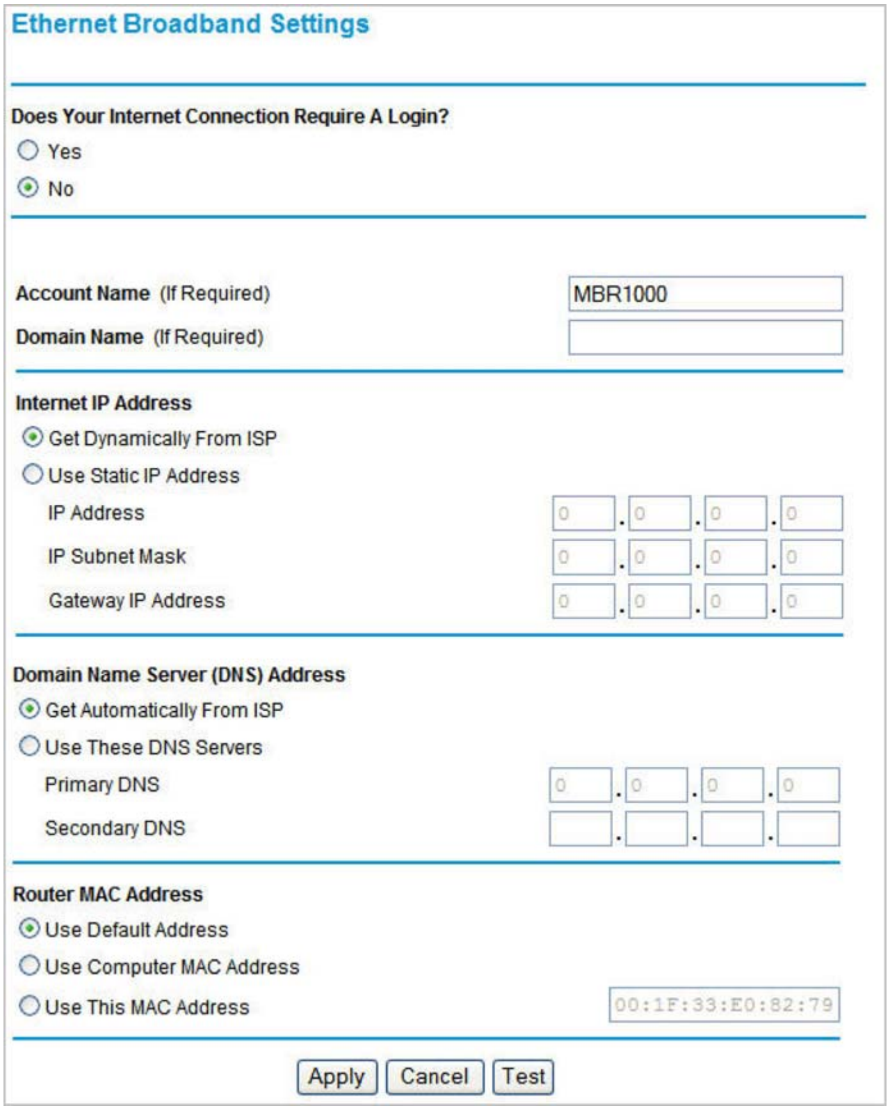


Table 5. Ethernet Broadband Settings Fields When Login Not Required

Fields and Check Boxes	Description
Account Name (If Required)	This is also known as the host name or system name. For most users, type your account name or user name in this field. For example, if your main mail account is JerAB@ISP.com, then put JerAB in this field. If your ISP has given you a specific host name, then type it (for example, CCA7324-A).
Domain Name (If Required)	For most users, you can leave this field blank, unless required by your ISP. You can type the domain name of your ISP. For example, if your ISP's mail server is mail.xxx.yyy.zzz, you would type xxx.yyy.zzz as the domain name. If you have a domain name given to you by your ISP, type it in this field. (For example, Earthlink Cable might require a host name of home, and Comcast sometimes supplies a domain name.) If you have a cable modem, this is usually the workgroup name.
Internet IP Address	If you log in to your service or your ISP did not provide you with a fixed IP address, the router finds an IP address for you automatically when you connect. Select **Get Dynamically From ISP**. If you have a fixed (or static IP) address, your ISP has provided you with the required information. Select **Use Static IP Address** and type the IP address, subnet mask and gateway IP address into the correct fields. For example: • **IP Address**. 24.218.156.183 • **Subnet Mask**. 255.255.255.0 • **Gateway IP Address**. 24.218.156.1
Domain Name Server (DNS) Address	The DNS server is used to look up site addresses based on their names. • If your ISP gave you one or two DNS addresses, select **Use These DNS Servers** and type the primary and secondary addresses. • Otherwise, select **Get Automatically From ISP**. **Note**: If you get “Address not found” errors when you go to a website, it is likely that your DNS servers are not set up correctly. You should contact your ISP to get DNS server addresses.
Router MAC Address	Your computer's local address is its unique address on your network. This is also referred to as the computer's MAC (Media Access Control) address. • Usually, select **Use Default MAC Address**. • If your ISP requires MAC authentication, then select either **Use Computer MAC Address** to disguise the router's MAC address with the computer's own MAC address, or **Use This MAC Address** to manually type the MAC address for a different computer. The format for the MAC address is XX:XX:XX:XX:XX:XX. This value might be changed if **Use Computer MAC Address** is selected once a value has already been set in the **Use This MAC Address** selection.

3. The following buttons are available:
   - **Apply**. Apply the changes that you made.
   - **Cancel**. Discard changes.
   - **Test**. Connect to the NETGEAR website. If you connect successfully, your settings work, and you can click **Logout** to exit these screens.

2. Wireless Network Configuration

For a wireless connection, the SSID, (also known as the wireless network name), and the wireless security settings must be the same for the router and wireless computers or wireless adapters. NETGEAR strongly recommends that you use wireless security.

The router is pre-configured with WPA-PSK/WPA2-PSK mixed mode and uses a unique SSID and passphrase. This information is printed on the label on the bottom of the router. Use this information to setup your WiFi computer and devices.

This chapter addresses the following:

- **Planning Your Wireless Network**
- **Manually Configure Your Wireless Settings**
- **Use Push 'N' Connect (WPS) to Configure Your Wireless Network**

Note: Computers can connect wirelessly at a range of several hundred feet. If you do not use wireless security, this can allow others outside your immediate area to access your network.

Planning Your Wireless Network

For compliance and compatibility between similar products in your area, the operating channel and region must be set correctly.

To configure the wireless network, you can either specify the wireless settings, or you can use Wi-Fi Protected Setup (WPS) to automatically set the SSID and implement WPA/WPA2 security.

- To manually configure the wireless settings, you must know the following:
  - SSID. The default SSID for the router is NETGEAR-3G.
  - The wireless mode (802.11n, 802.11g, or 802.11b) that each wireless adapter supports.
  - Wireless security option. To successfully implement wireless security, check each wireless adapter to determine which wireless security option it supports.

  See *Manually Configure Your Wireless Settings* on page 28.
- Push 'N' Connect (WPS) implements WPA/WPA2 wireless security on the router and your wireless computer or device at the same time. The wireless computer or device must be compatible with WPS.

  See *Use Push 'N' Connect (WPS) to Configure Your Wireless Network* on page 32.

Wireless Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the physical placement of the router. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

For best results, place your router according to the following guidelines:

- Near the center of the area in which your computers will operate.
- In an elevated location, such as a high shelf, where the wirelessly connected computers have line-of-sight access (even if through walls).
- Away from sources of interference, such as microwave ovens, and 2.4 GHz cordless phones (see *Interference Reduction Table* on page 100).
- Away from large metal surfaces.
- Put the antenna in a vertical position to provide the best side-to-side coverage. Put the antenna in a horizontal position to provide the best up-and-down coverage.
- If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Wireless Security Options

Indoors, computers can connect over 802.11n wireless networks at a maximum range of up to 300 feet. Such distances can allow others outside your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The Mobile Broadband 11n Wireless Router provides highly effective security features, which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

Each router is preconfigured for WPA-PSK/WPA2-PSK mixed-mode, and comes with a unique SSID and passphrase for each router.

There are several ways you can enhance the security of your wireless network:



Figure 1. Wireless Security

- **Restrict access based on MAC address**. You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the router. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn off the broadcast of the wireless network name (SSID)**. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies wireless network “discovery” feature of some products, such as Windows XP, but the data is still exposed.
- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK.
- **WPA-PSK (TKIP), WPA2-PSK (AES)**. Wi-Fi Protected Access (WPA) using a pre-shared key to perform authentication and generate the initial data encryption keys. The very strong authentication along with dynamic per frame re-keying of WPA makes it virtually impossible to compromise.

For more information about wireless technology, click the link to the online document *Wireless Networking Basics* in Appendix A.

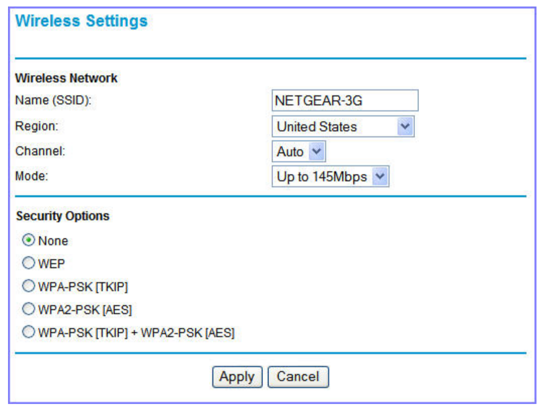
Manually Configure Your Wireless Settings

> **Note:** If you use a wireless computer to change the wireless network name (SSID) or wireless security, you will be disconnected when you click **Apply**. To avoid this occurrence, connect your computer directly to the router with an Ethernet cable while you are making changes.

To view or manually configure the wireless settings:

1. Log in to the router as described in *Log In to Your Router* on page 12.
2. Select Wireless Settings from the main menu.

   The settings for this screen are explained in *Table 6*.



3. Select the region in which the router will operate.
4. For initial configuration and test, leave the other settings unchanged.
5. To save your changes, click **Apply**.
6. Configure and test your computers for wireless connectivity.

   Set up your wireless computers with the same SSID and wireless security settings as your router. Check that they have a wireless link and are able to obtain an IP address by DHCP from the router. If there is interference, adjust the channel.

Table 1.

Settings		Description
Wireless Network	Name (SSID)	The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. When there is more than one wireless network, SSIDs provide a means for separating the traffic. To join a network, a wireless computer or device must use the SSID.
	Region	The location where the router is used.
	Channel	The wireless channel used by the gateway. The default is **Auto**. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, you might need to try different channels to see which works best.
	Mode	The default is Up to 145 Mbps.

Table 1.

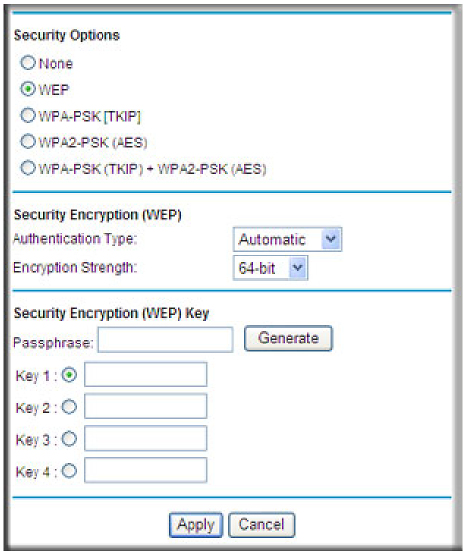
Settings		Description
Security Options	None	Use this setting to establish wireless connectivity before implementing wireless security. NETGEAR strongly recommends that you implement wireless security.
	WEP	Use encryption keys and data encryption for data security. You can select 64-bit or 128-bit encryption. See *Configuring WEP* on page 29.
	WPA-PSK (TKIP)	Allow only computers configured with WPA to connect to the router. See *Configuring WPA, WPA2, or WPA + WPA2* on page 31.
	WPA2-PSK (AES)	Allow only computers configured with WPA2 to connect to the router. See *Configuring WPA, WPA2, or WPA + WPA2* on page 31.
	WPA-PSK (TKIP) + WPA2-PSK (AES)	Allow computers configured with either WPA-PSK or WPA2-PSK security to connect to the router. See *Configuring WPA, WPA2, or WPA + WPA2* on page 31.

Configuring WEP

Note: If you use a wireless computer to configure wireless security settings, you will be disconnected when you click **Apply**. Reconfigure your wireless computer to match the new settings, or access the router from a wired computer to make further changes.

To configure WEP data encryption:

1. Log in to the router as described in *Log In to Your Router* on page 12.
2. From the main menu, select Wireless Settings to display the Wireless Settings screen.



3. In the Security Options section, select the **WEP** (Wired Equivalent Privacy) radio button:
4. Select the **Authentication Type setting**: **Automatic**, **Open System**, or **Shared Key**. The default is **Open System**.

   Note: *The authentication is separate from the data encryption. You can select authentication that requires a shared key, but still leaves data transmissions unencrypted. Security is stronger if you use both the Shared Key and WEP encryption settings.*

5. Select the **Encryption Strength** setting:
   - **64-bit**. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
   - **128-bit**. Enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).
6. Enter the encryption keys. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and access points in your network:
   - **Passphrase**. To use a passphrase to generate the keys, enter a passphrase, and click **Generate**. This automatically creates the keys. Wireless stations must use the passphrase or keys to access the router.

   Note: *Not all wireless adapters support passphrase key generation.*

   - **Key 1–Key4**. These values are *not* case-sensitive. You can manually enter the four data encryption keys. These values must be identical on all computers and access points in your network. Enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).
7. Select which of the four keys will be the default.

   Data transmissions are always encrypted using the default key. The other keys can be used only to decrypt received data. The four entries are disabled if WPA-PSK or WPA authentication is selected.
8. Click **Apply** to save your settings.

Configuring WPA, WPA2, or WPA + WPA2

Both WPA and WPA2 provide strong data security. WPA with TKIP is a software implementation that can be used on Windows systems with Service Pack 2 or later; WPA2 with AES is a hardware implementation; see your device documentation before implementing it. Consult the product documentation for your wireless adapter for instructions for configuring WPA settings.

> **Note:** If you use a wireless computer to configure wireless security settings, you will be disconnected when you click **Apply**. If this happens, reconfigure your wireless computer to match the new settings, or access the router from a wired computer to make further changes.

To configure WPA or WPA2 in the router:

1. Log in to the router as described in *Log In to Your Router* on page 12.
2. Select Wireless Settings from the main menu.
3. On the Wireless Setting screen, select the radio button for the WPA or WPA2 option of your choice.
4. For WPA-PSK or WPA2-PSK, enter the passphrase.
5. To save your settings, click **Apply**.

Use Push 'N' Connect (WPS) to Configure Your Wireless Network

To use Push 'N' Connect, your wireless computers or devices must support Wi-Fi Protected Setup (WPS). Compatible equipment usually has the WPS symbol on it. WPS can configure the network name (SSID) and set up WPA/WPA2 wireless security for the router and the wireless computer or device at the same time.

WPS considerations:

- NETGEAR's Push 'N' Connect feature is based on the WPS standard. All other Wi-Fi-certified and WPS-capable products should be compatible with NETGEAR products that implement Push 'N' Connect.
- If your wireless network will include a combination of WPS-capable devices and non-WPS-capable devices, NETGEAR suggests that you set up your wireless network and security settings manually first, and use WPS only for adding WPS-capable devices.

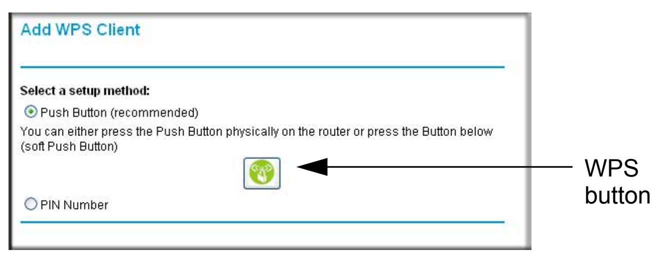
WPS Button

Any wireless computer or wireless adapter that will connect to the router wirelessly is a client. The client must support a WPS button, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart.

To use the router WPS button to add a WPS client:

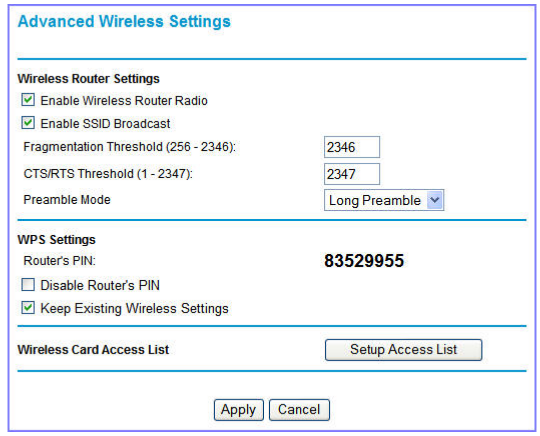
1. Log in to the router as described in *Log In to Your Router* on page 12.
2. On the router main menu, select Add WPS Client, and then click **Next**.

   By default, the **Push Button (recommended)** radio button is selected.



3. Either click the onscreen button or press the WPS button on the front of the router.

   The router tries to communicate with the client (the computer that wants to join the network) for 2 minutes.
4. Go to the client wireless computer, and run a WPS configuration utility. Follow the utility's instructions to click a WPS button.
5. Go back to the router screen to check for a message.



The router WPS screen displays a message confirming that the client was added to the wireless network. The router generates an SSID, and implements WPA/WPA2 wireless security. The router will keep these wireless settings unless you change them, or you clear the **Keep Existing Wireless Settings** check box in the Advanced Wireless Settings/WPS Settings screen.

6. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See *Manually Configure Your Wireless Settings* on page 28.

To access the Internet from any computer connected to your router, launch a browser such as Microsoft Internet Explorer or Mozilla Firefox. You should see the router’s Internet LED blink, indicating communication to the ISP.

Note: If no WPS-capable client devices are located during the 2-minute time frame, the SSID does not change, and no security is set up.

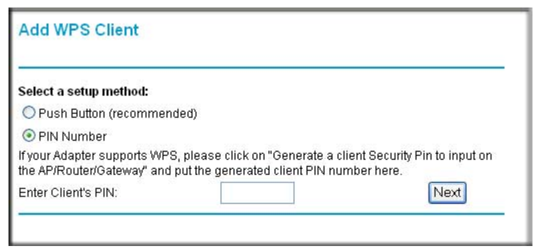
WPS PIN Entry

Any wireless computer or device that will connect to the router wirelessly is a client. The client must support a WPS PIN, and must have a WPS configuration utility, such as the NETGEAR Smart Wizard or Atheros Jumpstart.

The first time you add a WPS client, make sure that the **Keep Existing Wireless Settings** check box on the WPS Settings screen is cleared. This is the default setting for the router, and allows it to generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the router automatically selects this check box so that your SSID and wireless security settings stay the same if other WPS devices are added later.

To use a PIN to add a WPS client:

1. Log in to the router as described in *Log In to Your Router* on page 12.
2. On the router main menu, select Add WPS Client (computers that will connect wirelessly to the router are clients), and then click **Next**. The Add WPS Client screen displays.



3. Select the **PIN Number** radio button.
4. Go to the client wireless computer. Run a WPS configuration utility. Follow the utility's instructions to generate a PIN. Take note of the client PIN.
5. In the router Add WPS Client screen, enter the client PIN number, and then click **Next**.
   - The router tries to communicate with the client for 4 minutes. If no WPS clients connect during this time, the router wireless settings do not change.
   - The router WPS screen confirms that the client was added to the wireless network. The router generates an SSID, and implements WPA/WPA2 wireless security.
6. Note the new SSID and WPA/WPA2 password for the wireless network. You can view these settings in the Wireless Settings screen. See *Manually Configure Your Wireless Settings* on page 28.

To access the Internet from any computer connected to your router, launch an Internet browser such as Mozilla Firefox. You should see the router's Internet LED blink.

Add Wireless Computers That Do Not Support WPS

If you set up your network with WPS, and now you want to add a computer that does not support WPS, you must manually configure that computer. For information about how to view the wireless settings for the router, see *Manually Configure Your Wireless Settings* on page 28.

Because WPA randomly creates the SSID and WPA/WPA2 keys, they might be difficult to type or remember (that is one reason why the network is so secure). You can change the wireless settings so that they are easier for you to remember. If you do that, then you will need to set up the WPS-compatible computers again.

> **Note:** Making these changes will cause all wireless computers to be disconnected from network. You will then have to set them up with the new wireless settings.

To change wireless settings for the network:

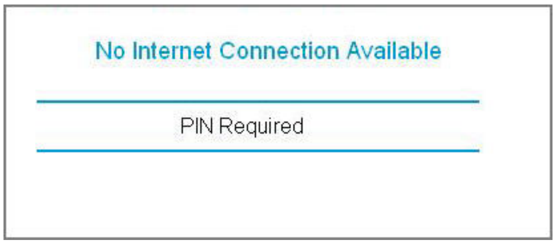
1. Use an Ethernet cable to connect a computer to the router. That way you will not get disconnected when you change the wireless settings.
2. Log in to the router and select Wireless Settings (see *Manually Configure Your Wireless Settings* on page 28).
3. Make the following changes:
   - Change the wireless network name (SSID) to a meaningful name.
   - On the WPA/PSK + WPA2/PSK screen, select a passphrase.
   - Make sure that the **Keep Wireless Settings** check box is selected in the WPS Settings screen so that your new settings will not be erased if you use WPS.
4. Click **Apply** so that your changes take effect. Write down your settings.

   All existing wireless clients are disassociated and disconnected from the router.
5. For the non-WPS devices that you want to connect, open the networking utility and follow the utility’s instructions to enter the security settings that you selected in Step 3 (the SSID, WPA/PSK + WPA2/PSK security method, and passphrase).
6. For the WPS devices that you want to connect, follow the procedure *WPS Button* on page 32 or *WPS PIN Entry* on page 34.

   The settings that you configured in Step 3 are broadcast to the WPS devices so that they can connect to the router.

SIM Card PIN Code

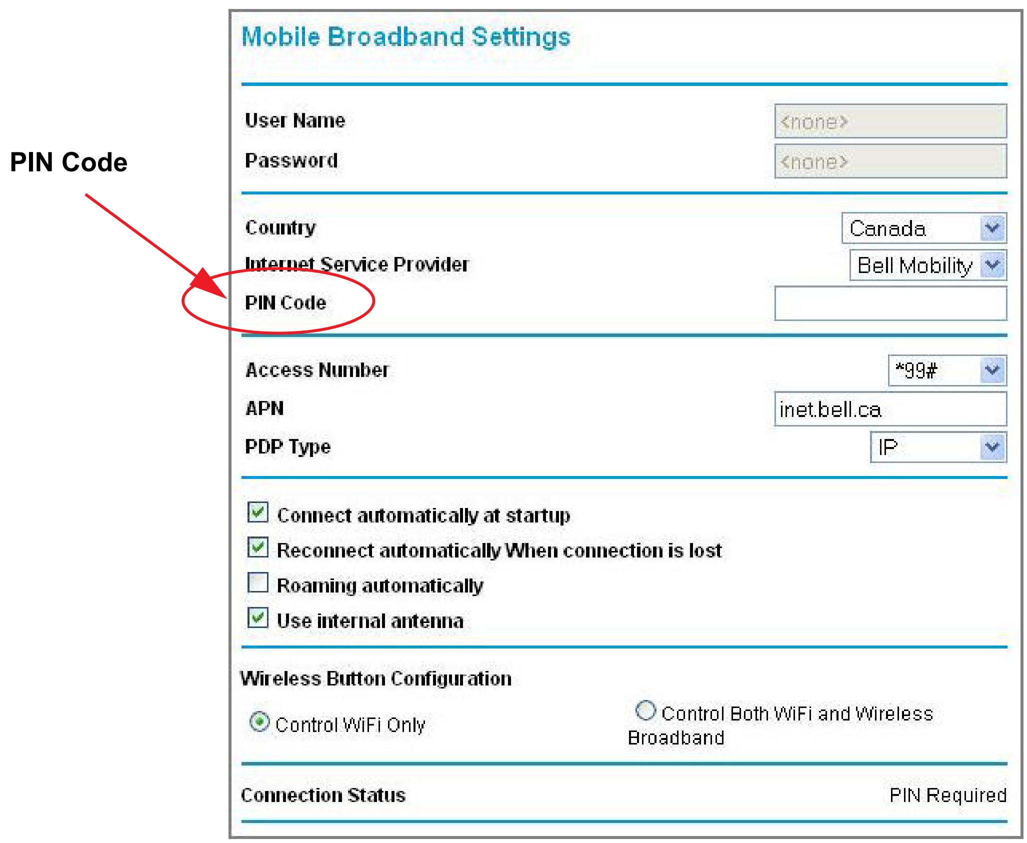
Some SIM cards may have a PIN code associated with them. Without the PIN code, you will not be able to access the internet. This status appears when a PIN is required, but has not yet been entered.



To enter the PIN code:

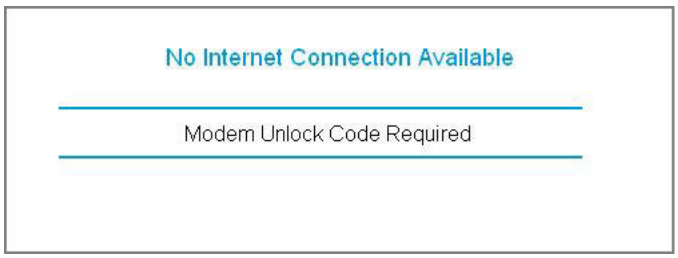
1. Log into the router and select **Mobile Broadband Settings** from the navigation tab.
2. Enter the PIN Code.

   Check with the router company if you do not know the PIN code.



SIM Card Modem Unlock Code

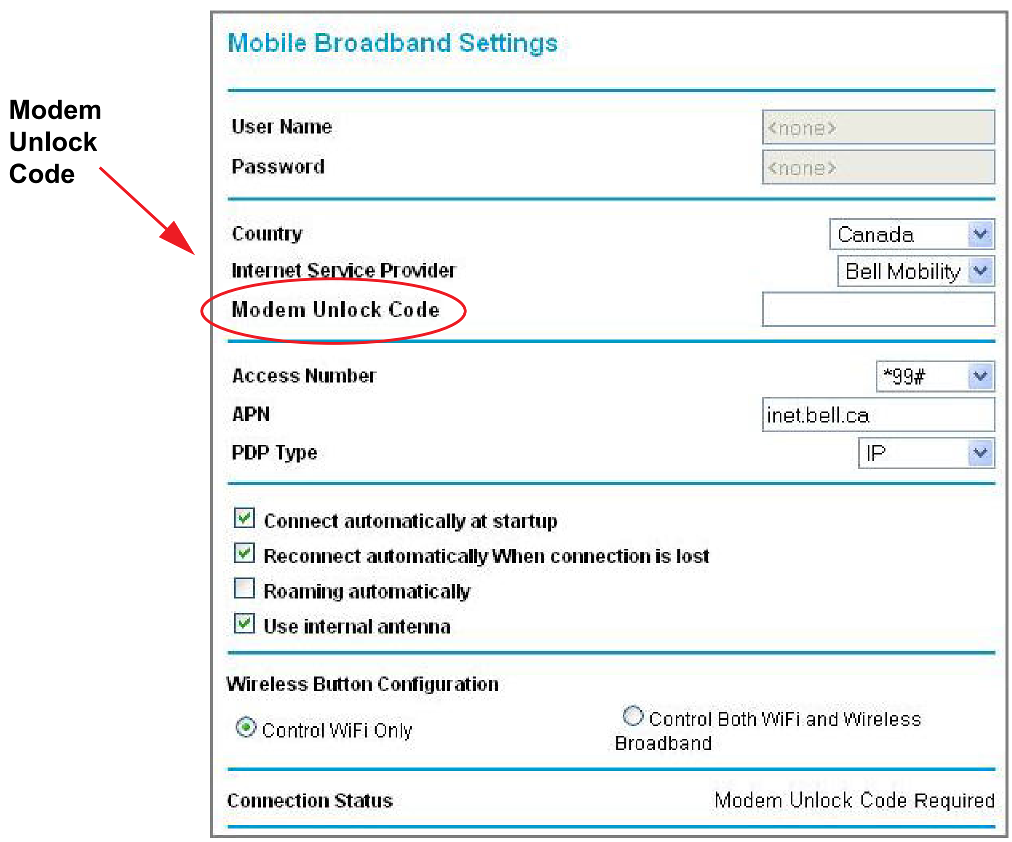
If you have a SIM card that is not provided by the company where you got the router, you might get an error indicating the modem is locked. To proceed, you must enter an unlock code.



To enter the modem unlock code:

1. Log into the router and select **Mobile Broadband Settings** from the navigation tab.
2. Enter the Modem Unlock Code.

   The modem unlock code can be obtained from the company that supplied the router.



3. Content Filtering 3

This chapter describes how to use the basic firewall features of the router to protect your network.

Note: For information about the advanced content filtering features port forwarding and port triggering, see *Port Forwarding and Port Triggering* on page 65.

Viewing, Selecting, and Saving Logged Information

The router logs security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enabled content filtering in the Block Sites screen, the Logs screen can show you when someone on your network tries to access a blocked site.

On the main menu, under Content Filtering, select Logs to display this screen:

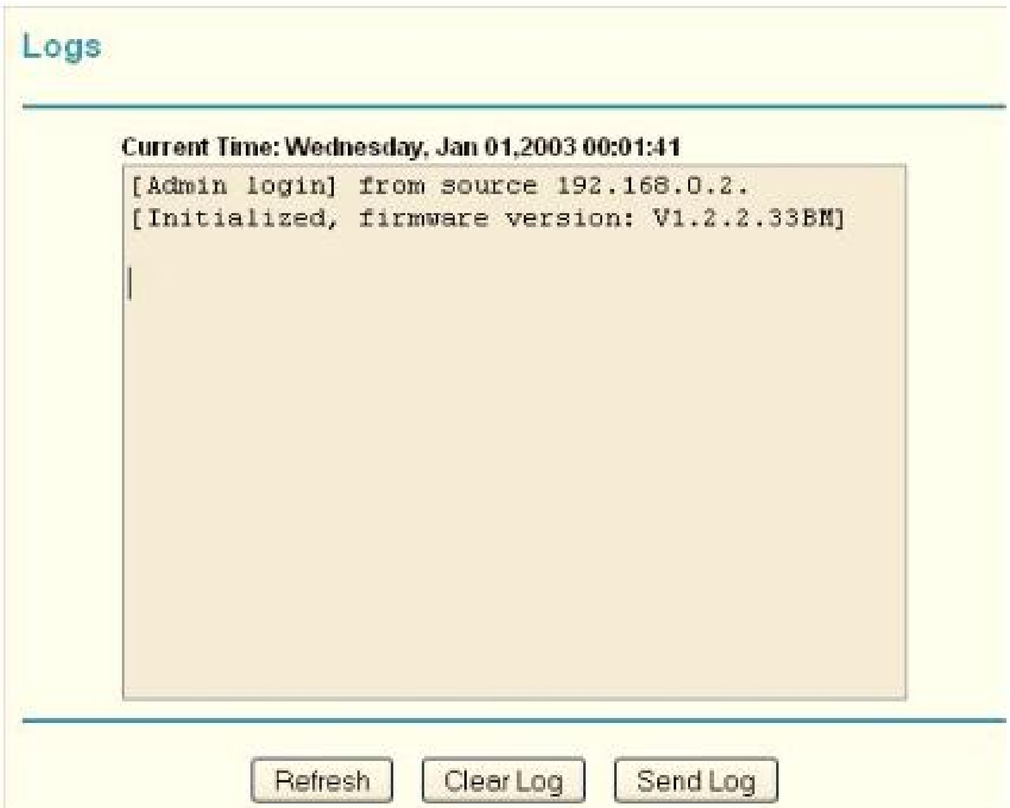


Figure 1.

Note: You can enable email notification to receive these logs in an email message. See *Enabling Security Event Email Notification* on page 46.

Log entries and action buttons are described in the *Table 7*.

Table 1.

Field or Button	Description
Current time	The date and time the log entry was recorded.
Description or action	The type of event and what action was taken, if any.
Source IP	The IP address of the initiating device for this log entry.
Source port and interface	The service port number of the initiating device, and whether it originated from the LAN or WAN.
Destination	The name or IP address of the destination device or website.
Destination port and interface	The service port number of the destination device, and whether it is on the LAN or WAN.
Refresh button	Refresh the log screen.
Clear Log button	Clear the log entries.
Send Log button	Email the log immediately.
Apply button	Apply the current settings.
Cancel button	Clear the current settings.

Selecting Which Information to Log

Besides the standard information listed previously, you can choose to log additional information. Those optional selections are as follows:

- Attempted access to blocked site
- Connections to the router menu
- Router operation (start up, get time, and so on)
- Known DoS attacks and port scans

Saving Log Files on a Server

You can choose to write the logs to a computer running a syslog program. To activate this feature, select to the **Broadcast on LAN** radio button, or enter the IP address of the server where the syslog file will be written.

Log Message Examples

Following are examples of log messages. In all cases, the log entry shows the time stamp as Day, Year-Month-Date Hour:Minute:Second.

Activation and Administration

```
Tue, 2002-05-21 18:48:39 - NETGEAR activated
```

This entry indicates a power-up or reboot with initial time entry.

`Tue, 2002-05-21 18:55:00 - Administrator login successful - IP:192.168.0.2`

`Thu, 2002-05-21 18:56:58 - Administrator logout - IP:192.168.0.2`

This entry shows an administrator logging in to and out from IP address 192.168.0.2.

```
Tue, 2002-05-21 19:00:06 - Login screen timed out - IP:192.168.0.2
```

This entry shows a time-out of the administrator login.

```
Wed, 2002-05-22 22:00:19 - Log emailed
```

This entry shows when the log was emailed.

Dropped Packets

```
Wed, 2002-05-22 07:15:15 - TCP packet dropped - Source:64.12.47.28,4787,WAN -
Destination:134.177.0.11,21,LAN - [Inbound Default rule match]
```

```
Sun, 2002-05-22 12:50:33 - UDP packet dropped - Source:64.12.47.28,10714,WAN -
Destination:134.177.0.11,6970,LAN - [Inbound Default rule match]
```

```
Sun, 2002-05-22 21:02:53 - ICMP packet dropped - Source:64.12.47.28,0,WAN -
Destination:134.177.0.11,0,LAN - [Inbound Default rule match]
```

These entries show an inbound FTP (port 21) packet, User Datagram Protocol (UDP) packet (port 6970), and Internet Control Message Protocol (ICMP) packet (port 0) being dropped as a result of the default inbound rule, which states that all inbound packets are denied.

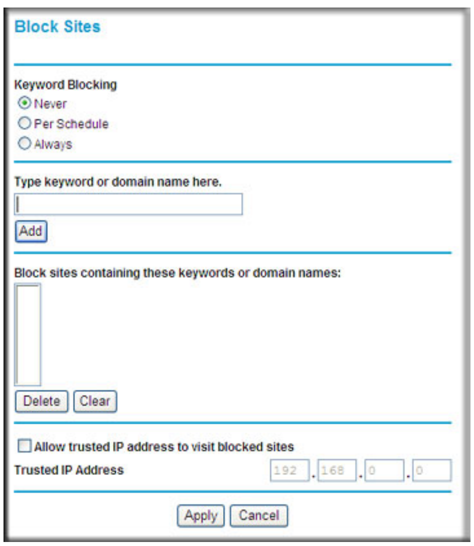
Blocking Sites and Keywords

The router provides a variety of options for blocking Internet-based content and communications services. With its content filtering feature, the router prevents objectionable content from reaching your PCs. You can control access to Internet content by screening for keywords within Web addresses. Content filtering options include:

- Keyword blocking of HTTP traffic.
- Outbound service blocking. Limits access from your LAN to Internet locations or services that you specify as off-limits.
- Denial of service (DoS) protection. Detects and thwarts DoS attacks such as Ping of Death, SYN flood, LAND attack, and IP spoofing.
- Blocking unwanted traffic from the Internet to your LAN.

The router allows you to restrict access to Internet content based on Web addresses and Web address keywords.

1. Log in to the router as described in *Log In to Your Router* on page 12.
2. On the main menu, select Block Sites to display the Block Sites screen:



3. To enable keyword blocking, select one of the following:
   - **Per Schedule**. Turn on keyword blocking according to the settings on the Schedule screen.
   - **Always**. Turn on keyword blocking all the time, independent of the setting in the Schedule screen.
4. Enter a keyword or domain in the **Keyword** field, click **Add Keyword**, and then click **Apply**.

Some examples of keyword applications are shown in the following chart.

Table 2.

Keyword	Result
XXX	Block the URL http://www.badstuf.com/xxx.html.
.com	Only websites with other domain suffixes (such as .edu or .gov) can be viewed.
. (a period)	Block all Internet browsing access.

Up to 32 entries are supported in the Keyword list.

Note: If you block sites, you can set up the router to log attempts to access them. See *Viewing, Selecting, and Saving Logged Information* on page 39.

5. To delete a keyword or domain, select it from the list, click **Delete Keyword**, and then click **Apply**.
6. To specify a trusted user, enter that computer's IP address in the **Trusted IP Address** field, and then click **Apply**.

   You can specify one trusted user, which is a computer that will be exempt from blocking and logging. Since the trusted user will be identified by an IP address, you should configure that computer with a fixed IP address.
7. Click **Apply** to save your settings.

Blocking Services

1. Log in to the router as described in *Log In to Your Router* on page 12.
2. In the main menu, under Content Filtering, select Block Services to display this screen:

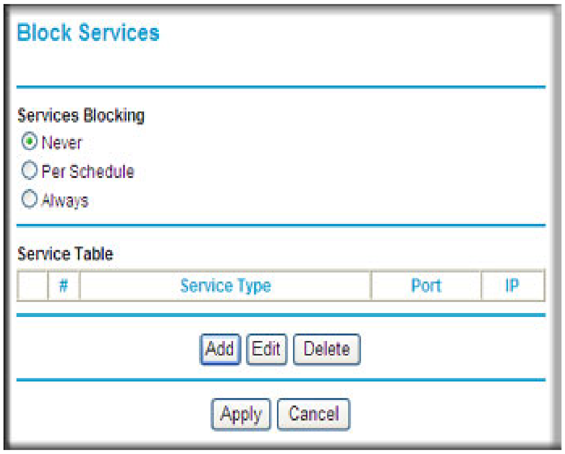


Figure 2.

3. Select one of the following:
   - **Per Schedule**. Turn on keyword blocking according to the settings in the Schedule screen.
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule screen.
4. Click **Add**, and the following screen displays:

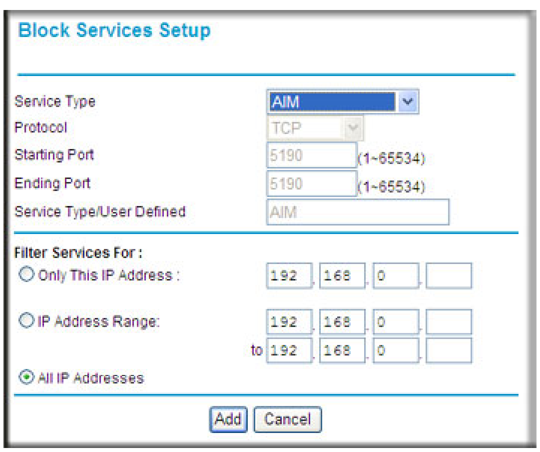


Figure 3.

5. Either select a service from the **Service Type** drop-down list, or use the **Service/Type User Defined** field to create a custom service.
6. Click **Add** to create the service, and it will be listed in the Service Table on the Block Services screen.
7. Click **Apply** to save your settings.

Scheduling

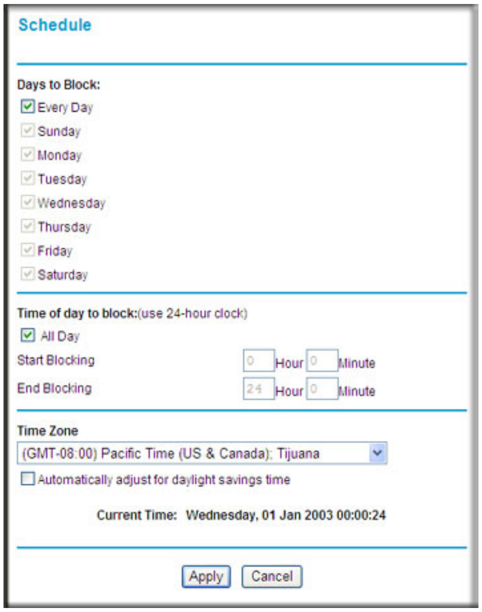
The router uses Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet.

Setting Your Time Zone

To localize the time for your log entries, you must specify your time zone:

1. Log in to the router as described in *Log In to Your Router* on page 12.
2. On the main menu under Content Filtering, select Schedule:
3. Select your time zone. This setting will be used for the blocking schedule according to your local time zone and for time-stamping log entries.

   If your time zone is currently in daylight savings time, select the **Automatically adjust for daylight savings time** check box.
4. Click **Apply** to save your settings.



Scheduling Firewall Services

If you enabled service blocking in the Block Services screen or port forwarding in the Ports screen, you can set up a schedule for when blocking occurs or when access is not restricted.

1. Log in to the router as described in *Log In to Your Router* on page 12.
2. On the main menu, select the Schedule. The Schedule screen appears.
3. To block Internet services based on a schedule, select **Every Day**, or select one or more days. If you want to limit access completely for the selected days, select **All Day**. Otherwise, to limit access during certain times for the selected days, fill in the **Start Blocking** and **End Blocking** fields.
4. Enter the values in 24-hour time format. For example, 10:30 a.m. would be 10 hours and 30 minutes, and 10:30 p.m. would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule will be effective through midnight the next day.
5. Click **Apply** to save your changes.

Enabling Security Event Email Notification

To set up the router so that you can receive logs and alerts by email, select Email from the router menu to display the following screen:



To receive alerts and logs by email:

1. Select the **Turn Email Notification On** check box.
2. Fill in the fields to send alerts and logs through email.
   - **Your Outgoing Mail Server**. Enter the name or IP address of the outgoing SMTP mail server of your ISP (such as mail.myISP.com).
   - **Send to This Email Address.** Enter the e-mail address where you want to send the alerts and logs. Use a full email address, such as ChrisXY@myISP.com.
   - **My mail server requires authentication**. Select this check box if you need to log in to your SMTP server to send email. If you select this feature, you must enter the user name and password for the mail server.

   Tip: If you cannot remember this information, check the settings in your email program.

3. Specify when you want the alerts and logs to be sent:
   - **Send alert immediately**. Select the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
   - **Send logs according to this schedule**. Specifies how often to send the logs: **Hourly**, **Daily**, **Weekly**, or **When Full**.
   - **Day for sending log**. Specifies which day of the week to send the log. Relevant when the log is sent weekly.
   - **Time for sending log**. Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

   If the **Weekly**, **Daily**, or **Hourly** option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified email address. After the log is sent, it is cleared from the router's memory. If the router cannot e-mail the log file, the log buffer might fill up. In this case, the router overwrites the log and discards its contents.
4. Click **Apply** so that your changes take effect.

Managing Your Network

4

This chapter describes how to perform network management tasks with your Mobile Broadband 11n Wireless Router.

- **Router Status**
- **Backing Up, Restoring, or Erasing Your Settings**
- **Protecting Access to Your Router**
- **Running Diagnostic Utilities and Rebooting the Router**
- **Upgrading the Router Firmware**

Router Status

From the main menu, under Maintenance, select Router Status to view this screen.

You can use this screen to view the status of the router, to show statistics, or to view the connection status.

- For information about the fields on this screen, see *Table 9*.
- See *Showing Statistics* on page 50 for information about statistics.
- For information about the Internet connection, see *Connection Status* on page 51.

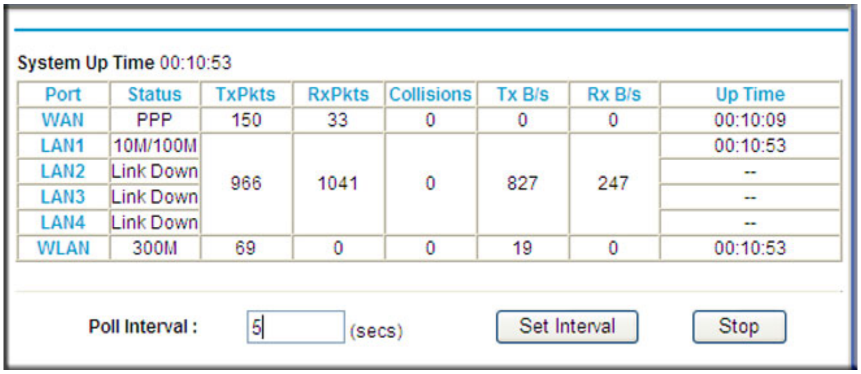


Table 1.

Field		Description
Firmware Version		This field displays the router firmware version.
Mobile Broadband	Modem Identity	Shows the modem in use.
	Modem sw version	The software version of the modem.
	Modem driver version	The driver version of the modem.
	IMSI	International Mobile Subscriber Identity. SIM card identity.
	IMEI	International Mobile Equipment Identity. Unique identity of the modem.
	Operator	The ISP for the broadband wireless network.
	Network mode	The mode of the current network the modem is connected to. This is dependent on coverage and distance from the cell site.
WAN Port	Connection Status	The status of the Internet connection.
	IP Address	The IP address used by the modem. If no address is shown, the router cannot connect to the Internet.
	Protocol	The protocol for the Internet connection, which is PPP (Point-to-Point).
	IP Subnet Mask	The IP subnet mask used by the router's USB port.
	Gateway IP Address	The IP address used by the router.
	Domain Name Server	The DNS server IP addresses used by the router. These addresses are usually obtained dynamically from the ISP.
LAN Port	MAC Address	The Ethernet MAC address used by the router's LAN port.
	IP Address	The LAN port IP address. The default is 192.168.0.1.
	DHCP	• **Off.** The router does not assign IP addresses to PCs on the LAN. • **On.** The router assigns IP addresses to PCs on the LAN.
	IP Subnet Mask	The LAN port IP subnet mask. The default is 255.255.255.0.
Wireless Port (See *Manually Configure Your Wireless Settings* on page 28.	Name (SSID)	The service set ID, also known as the wireless network name.
	Region	The country where the unit is set up for use.
	Channel	The current channel, which determines the operating frequency.
	Wireless AP	Indicates if the access point feature is disabled or not. If not enabled, the Wireless LED on the front panel will be off.
	Broadcast Name	Indicates if the router is configured to broadcast its SSID.

Showing Statistics

Click the **Show Statistics** button on the Router Status screen to display router usage statistics:



System Up Time 00:10:53

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	PPP	150	33	0	0	0	00:10:09
LAN1	10M/100M	966	1041	0	827	247	00:10:53
LAN2	Link Down						--
LAN3	Link Down						--
LAN4	Link Down						--
WLAN	300M	69	0	0	19	0	00:10:53

Poll Interval : 5 (secs) Set Interval Stop

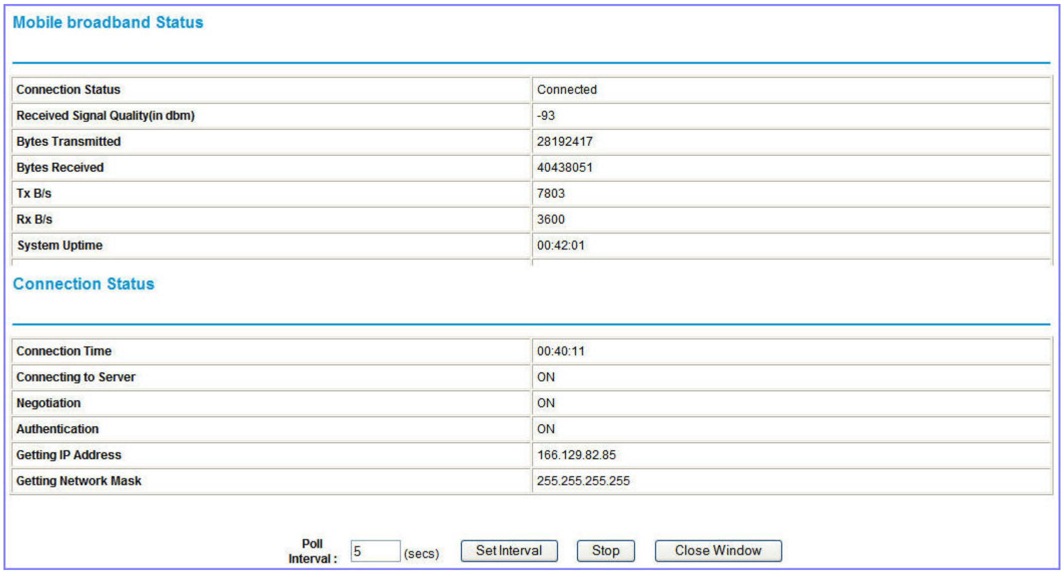
Table 10 explains the statistic fields.

Table 2.

Field	Description
Status	The link status. Note that LAN2, LAN3, and LAN4 are guest networks.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The average egress line utilization for this port.
Rx B/s	The average □□□□□□□□□for this port□□□□□□□□□□
Up Time	The time elapsed since the last power cycle or reset.

Connection Status

Click the **Connection Status** button on the Router Status screen:



This screen shows the following statistics:

Table 3.

Field		**Description**
Mobile Broadband Service	Connection Status	The status of the Internet connection. • **Scanning**. The modem is scanning for broadband wireless networks in your area. • **Connected**. The router is connected to the Internet. • **No USB Device Attached** . The router does not detect a USB modem connected to its USB port. Either the modem is disconnected, or it is not correctly seated. To correct the problem remove the modem and reinsert it into the port.
	Received Signal Quality (in dBm)	Modem radio reception. A small, negative number indicates good signal quality.
	Bytes Transmitted	The number of bytes transmitted in the most recent connection session.
	Bytes Received	The number of bytes received in the most recent connection session.
	Tx B/s	The transmission rate.
	Rx B/s	The receiving rate.
	System Uptime	Time elapsed since the last reboot.

Table 3.

Field		Description
Connection Status	Connection Time	The time elapsed since the last connection to the Internet through the broadband port.
	Connecting to Server	The connection status.
	Negotiation	Success or Failed.
	Authentication	Success or Failed.
	Getting IP Address	The IP address assigned to the WAN port by the ADSL Internet Service Provider.
	Getting Network Mask	The network mask assigned to the WAN port by the ADSL Internet Service Provider.

Viewing Attached Devices

The Attached Devices screen shows all IP devices that the router discovered on the local network. From the main menu, under Maintenance, select Attached Devices:



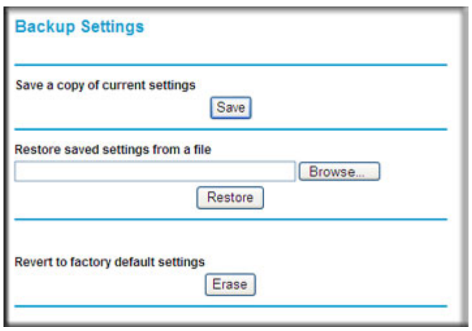
For each device, the table shows the IP address, device name if available, and the Ethernet MAC address. If the router is rebooted, this data is lost until the router rediscovers the devices. To force the router to look for attached devices, click the **Refresh** button.

Backing Up, Restoring, or Erasing Your Settings

The configuration settings of the router are stored in a configuration file in the router. This file can be backed up to your computer, restored, or reverted to factory default settings. The procedures in the following sections explain how to do these tasks.

Backing Up the Configuration to a File

1. Log in to the router. Type **http://www.routerlogin.net** in the address field of your Internet browser. Enter **admin** for the user name and your password (or the default, **password**).
2. Under Maintenance on the main menu, select Backup Settings to display the Backup Settings screen.



3. Click **Save** to save a copy of the current settings.
4. Store the .cfg file on a computer on your network.

Restoring the Configuration from a File

To restore the configuration:

1. Log in to the router. Type **http://www.routerlogin.net** in the address field of your Internet browser. Enter **admin** for the user name and your password (or the default, **password**).
2. Under Maintenance on the main menu, select Backup Settings.
3. Enter the full path to the file on your network, or click **Browse** to locate the file.
4. When you have located the .cfg file, click **Restore** to upload the file to the router.

   The router reboots.

Erasing the Configuration

You can use the Erase feature to erase its configuration settings and restore the router to the factory default settings.

To erase the configuration:

1. Under Maintenance on the main menu, select Backup Settings.
2. Click **Erase**.

   The router reboots.

   After an erase, the router password is **password**, the LAN IP address is **192.168.0.1**, and the router DHCP client is enabled.

Note: To restore the factory default settings when you do not know the login password or IP address, press the Restore Factory Settings button on the bottom of the router for 6 seconds.

Protecting Access to Your Router

For security reasons, the router has its own user name and password. Also, after a period of inactivity, the login automatically disconnects. The user name and password are not the same as a user name or password you might use to log in to your Internet connection.

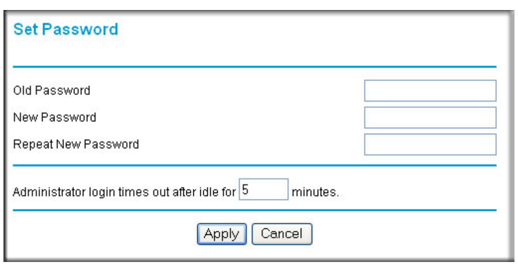
NETGEAR recommends that you change this password to a more secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of both uppercase and lowercase letters, numbers, and symbols. Your password can be up to 30 characters.

Changing the Built-In Password

1. To log in to the router, type **http://www.routerlogin.net** in the address field of your Internet browser. Enter **admin** for the user name and your password (or the default, **password**).

> **Note:** If you changed the password and do not remember what it is, you can reset the router to its factory default settings. See *Restoring the Default Configuration and Password* on page 91.

2. From the main menu, under Maintenance, select Set Password.



3. To change the password, first enter the old password, and then enter the new password twice.
4. Click **Apply** to save your changes.

> **Note:** After changing the password, you must log in again to continue the configuration. If you have backed up the router settings previously, you should do a new backup so that the saved settings file includes the new password.

Changing the Administrator Login Time-Out

For security, the administrator login to the router configuration times out after a period of inactivity. To change the login time-out period:

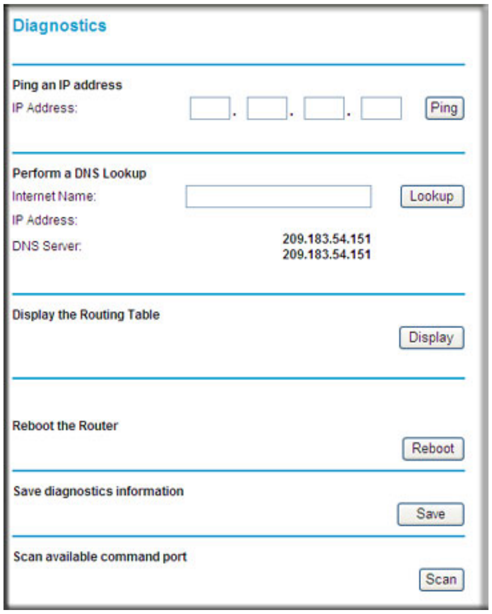
1. In the Set Password screen, type a number in the **Administrator login times out** field. The suggested default value is 5 minutes.
2. Click **Apply** to save your changes, or click **Cancel** to keep the current period.

Running Diagnostic Utilities and Rebooting the Router

The router has a diagnostics feature. You can use the Diagnostics screen to perform the following functions from the router:

- Ping an IP address to test connectivity to see if you can reach a remote host. If Ping VPN is enabled, the ping packet always goes through the VPN if the VPN tunnel is enabled and working.
- Perform a DNS lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.
- Display the routing table to identify what other routers the router is communicating with.
- Reboot the router to enable new network configurations to take effect or to clear problems with the router's network connection.

From the main menu, under Maintenance, select Diagnostics.



- **Ping**. Ping an IP address.
- **Lookup**. A Domain Name Server (DNS) converts the Internet name such as www.netgear.com to an IP address. If you need the IP address of a server on the Internet, you can do a DNS lookup to find the IP address.
- **Display**. View the internal routing table. Typically, this information is used only by Technical Support.
- **Reboot**. Shut down and restart the router.

  If you reboot the router you will lose your connection. To access the router you will need to log in again after it has finished rebooting.
- **Save**. Save diagnostic information.

Upgrading the Router Firmware

The router firmware is stored in flash memory, and can be upgraded as new firmware is released by NETGEAR. Upgrade files can be downloaded from the NETGEAR web site. If the upgrade file is compressed (a .zip file), you must first extract the binary (.bin or .img) file before uploading it to the router.

NETGEAR recommends that you back up your configuration before doing a firmware upgrade. After the upgrade is complete, you might need to restore your configuration settings.

1. Download and unzip the new firmware file from NETGEAR.

   The Web browser used to upload new firmware into the router must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer 5.0 or later, or Mozilla Firefox 2.0 or later.

2. Log in to the router. Type **http://www.routerlogin.net** in the address field of your Internet browser. Enter **admin** for the user name and your password (or the default, **password**).
3. From the main menu, under Maintenance, select Router Upgrade to display this screen.



4. Click **Browse** to locate the binary (.bin or .img) upgrade file.
5. Click **Upload**.

WARNING!

When uploading firmware to the router, do not interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it might corrupt the firmware, causing router to be unworkable and inaccessible. When the upload is complete, your router will automatically restart. The upgrade process typically takes about 1 minute. In some cases, you might need to clear the configuration and reconfigure the router after upgrading.

5. Advanced

5

This chapter describes how to configure the advanced features of your Mobile Broadband 11n Wireless Router.

- **SIM Settings**
- **Advanced Wireless Settings**
- **Wireless Repeating Function**
- **Port Forwarding and Port Triggering**
- **WAN Setup**
- **LAN Setup**
- **QoS Setup**
- **Dynamic DNS**
- **Using Static Routes**
- **Enabling Remote Management**
- **Universal Plug and Play**
- **Traffic Meter**

SIM Settings

From the main menu, select SIM Settings to display the following screen:

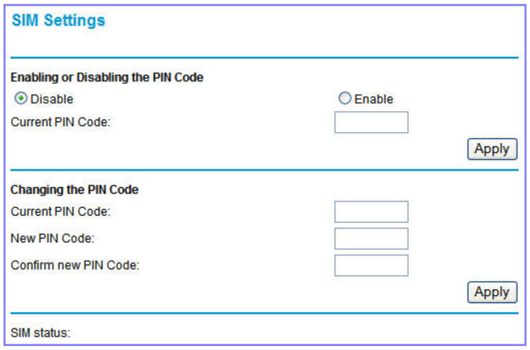


Table 1.

Field	Description
Enabling or Disabling the PIN Code	Controls whether the PIN code on the SIM card will be used to connect to the network.
Changing the PIN Code	Changes the PIN code on the SIM card.
SIM status	Current SIM card access status.

Advanced Wireless Settings

From the main menu, select Advanced Wireless Settings to display the following screen:



Table 2.

Field	Description
Enable Wireless Router Radio	Selected by default, this setting enables the wireless radio, which allows the router to work as a wireless access point. Turning off the wireless radio can be helpful for configuration, network tuning, or troubleshooting.
Fragmentation Length, CTS/RTS Threshold, and Preamble Mode	These should be left at their default settings.
Router PIN	The PIN number used for Push 'N' Connect.
Disable Router PIN	By default, this check box is cleared. This allows the WPS clients to discover the router's PIN.
Keep Wireless Settings	By default, this check box is cleared. This allows the router to automatically generate the SSID and WPA/WPA2 security settings when it implements WPS. After WPS is implemented, the router automatically selects the **Keep Existing Wireless Settings** check box so that your SSID and wireless security settings remain the same if other WPS-enabled devices are added later.
Turn Access Control On	Access control is disabled by default so that any computer configured with the correct SSID can connect. See *Restricting Access by MAC Address* on page 62.

Wireless Station Access Control

By default, any wireless PC configured with the correct SSID and wireless security settings is allowed access to your wireless network. You can use wireless access point settings in the Wireless Setting screen to further restrict wireless access to your network:

- **Turn off wireless connectivity completely**.
  You can completely turn off the wireless portion of the router. For example, if you use your notebook computer to wirelessly connect to your router, and you take a business trip, you can turn off the wireless portion of the router while you are traveling. Other members of your household who use computers connected to the router via Ethernet cables can still use the router. To do this, clear the **Enable Wireless Router Radio** check box on the Wireless Settings screen, and then click **Apply**.
- **Hide your wireless network name (SSID)**.
  By default, the router is set to broadcast its wireless network name (SSID). You can restrict wireless access to your network by not broadcasting the wireless network name (SSID). To do this, clear the **Enable SSID Broadcast** check box on the Wireless Settings screen, and then click **Apply**. Wireless devices will not “see” your router. You must configure your wireless devices to match the wireless network name (SSID) of the router.

Note: The SSID of any wireless access adapters must match the SSID you configure in the router. If they do not match, you will not get a wireless connection to the router.

Restricting Access by MAC Address

For increased security, you can restrict access to the wireless network to allow only specific PCs based on their MAC addresses. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the Mobile Broadband 11n Wireless Router. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

Note: If you configure the router from a wireless computer, add your computer’s MAC address to the access list. Otherwise you will lose your wireless connection when you click **Apply**. You must then access the router from a wired computer, or from a wireless computer that is on the access control list, to make any further changes.

To restrict access based on MAC addresses:

1. From the main menu, under Advanced, select Wireless Settings. Click **Setup Access List** to display the Wireless Station Access List screen.



2. Select **Turn Access Control On** check box. Adjust the list as needed for your network. You can add devices to the Trusted Wireless Stations list. Click **Add** to display the following screen:



3. You can add devices to the list using either of the following methods:
   - If the computer is in the Available Wireless Cards table, select its radio button to capture its MAC address.
   - Use the Wireless Card Entry fields to enter the MAC address of the device to be added. The MAC address can usually be found on the bottom of the wireless device.
   - If no device name appears when you enter the MAC address, you can type a descriptive name for the computer that you are adding.
4. Click **Apply** to save these settings. Now, only devices on this list will be allowed to wirelessly connect to the router.

Wireless Repeating Function

From the main menu, select Wireless Repeating Function to display the following screen:

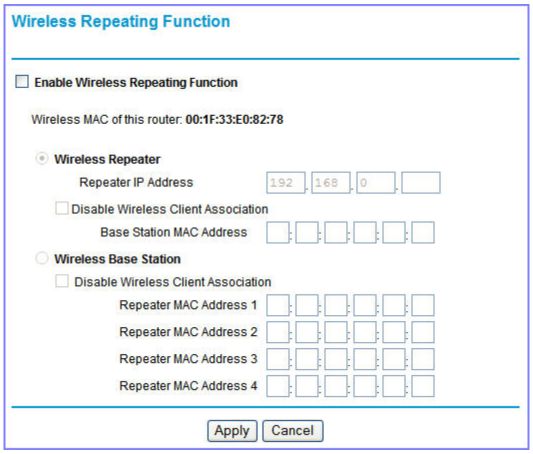


Table 3.

Field	Description
Enable Wireless Repeating	Enable this if you wish to use either Bridge mode or Repeater mode, and then select the mode you want for your environment. • **Wireless Repeater**. In this mode, the MBR1210 will communicate *only* with another Base Station–mode wireless station. You must enter the MAC address (physical address) of the other Base Station–mode wireless station in the field provided. WEP / WPA-PSK [TKIP] can (and should) be used to protect this communication. • **Wireless Base Station** . Select this only if this MBR1210 is the "master" for a group of Repeater-mode wireless stations. The other Repeater–mode wireless stations must be set to Wireless Repeater–mode, using this MBR1210's MAC address. They then send all traffic to this master, rather than communicate directly with each other. WEP / WPA-PSK [TKIP] can (and should) be used to protect this traffic. If this option is selected, you must enter the MAC addresses of the other access points in the fields provided.

Port Forwarding and Port Triggering

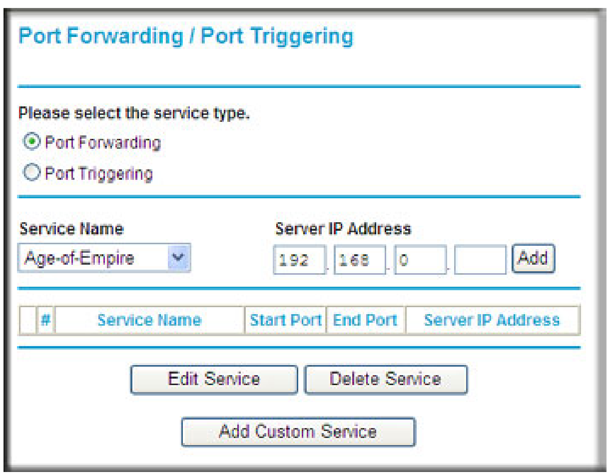
Port forwarding and port triggering are advanced features that affect the behavior of the firewall in your router. In the Port Forwarding / Port Triggering screen, you can make local computers or servers available to the Internet for different services (for example, FTP or HTTP), to play Internet games (like Quake III), or to use Internet applications (like CU-SeeMe).

- Port forwarding is designed for FTP, Web server, or other server-based services. Once port forwarding is set up, requests from the Internet are forwarded to the correct server.
- Port triggering monitors outbound traffic. When the router detects traffic on the specified outbound port, it remembers the IP address of the computer that sent the data and triggers the incoming port. Incoming traffic on the triggered port is then forwarded to the triggering computer. Port triggering allows requests from the Internet only after a designated port is triggered. Port triggering applies to chat and Internet games.

Port Forwarding

To set up port forwarding:

1. From the main menu, under Advanced, select Port Forwarding/Port Triggering. The following screen displays:



By default, the **Port Forwarding** radio button is selected.

2. You can select a service or create a custom service.
   - Select a service from the **Service Name** drop-down list and specify the computer's IP address.
   - If you want to add a service that is not in the list, click the **Add Custom Service** button. Fill in the fields in the Add Custom Service screen.

The service appears in the list.

Port Triggering

To set up port triggering:

1. From the main menu, under Advanced, select Port Forwarding/Port Triggering.
2. Select the **Port Triggering** radio button to display the following screen:



3. Click **Add Service** and fill in the fields in the Add Service screen.

   The service appears in the list. For more detailed information, see the Port Forwarding/Port Triggering help.

WAN Setup

To change broadband Internet connection settings, use the Broadband Settings screen, as described in *Manually Configure Your Internet Settings* on page 15.

To view or change the WAN setup:

1. From the main menu, select WAN Setup to display the WAN Setup screen.
2. Make the changes that you want, and then click **Apply** to save the settings.

The WAN Setup fields are described in the table below.

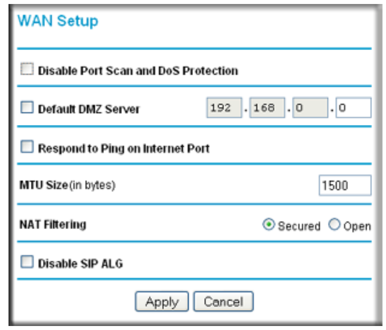


Table 4.

Setting	Description
Disable SPI Firewall	This check box is usually cleared so that the firewall protects your LAN against port scans and denial of service attacks. This check box should be selected only in special circumstances.
Default DMZ Server	This feature is sometimes helpful when you are using some online games and videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See *Setting Up a Default DMZ Server* on page 68.
Respond to Ping on Internet	If you want the router to respond to a ping from the Internet, select this check box. This should be used only as a diagnostic tool, since it allows your router to be discovered. Do not select this check box unless you have a specific reason to do so.
MTU Size	Maximum Transmit Unit (MTU) value. For most Ethernet networks this is 1500 bytes, or 1492 bytes for PPPoE connections, or 1436 bytes for PPTP connections.
NAT Filtering	This is set to **Secured** to provide a secure firewall to protect computers on the LAN from attacks from the Internet. The Open setting is less secure.
Disable SIP ALG	Some VoIP applications do not work well with SIP ALG. Selecting this check box might help your VoIP devices create or accept a call through the router.

Setting Up a Default DMZ Server

WARNING!

For security reasons, you should avoid using the default DMZ server feature. When a computer is designated as the default DMZ server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with NAT. The router is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server.

Incoming traffic from the Internet is normally discarded by the router unless the traffic is a response to one of your local computers or a service that you have configured in the Ports screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

To assign a computer or server to be a default DMZ server:

1. Go to the WAN Setup screen as described in the previous section.
2. Select the **Default DMZ Server** check box.
3. Type the IP address for that server.
4. Click **Apply** to save your changes.

LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as DHCP and RIP. These features can be found under Advanced in the router main menu.

The router is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The router default LAN IP configuration is:

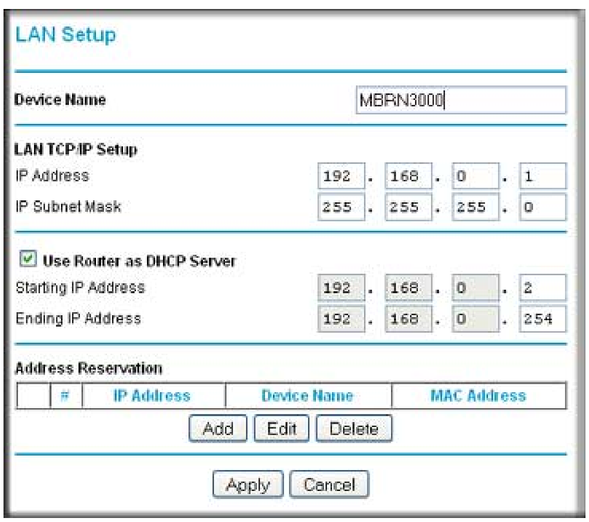
- LAN IP address. 192.168.0.1
- Subnet mask. 255.255.255.0

These addresses are part of the Internet Engineering Task Force (IETF)–designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in this screen.

> **Tip:** If you change the LAN IP address of the router while connected through the browser, you will be disconnected, and so will others connected to the router. To connect to the router, you must open a new connection to the new IP address and log in again. Others using the router must restart their computers to connect to the router again.

To view or change the LAN setup:

1. Select LAN IP to display the LAN Setup screen.



2. Change the settings. For more information, see *DHCP Settings* on page 70, or *Reserved IP Addresses* on page 71.
3. Click **Apply** to save the changes.

The LAN TCP/IP Setup parameters are explained in the table below.

Table 5.

Settings		Description
Device Name		
LAN TCP/IP Setup	IP Address	The LAN IP address of the router.
	IP Subnet Mask	The LAN subnet mask of the router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.
DHCP Server For more information, see *DHCP Settings* on page 70.	Use Router as a DHCP Server	This check box is usually selected so that the router functions as a Dynamic Host Configuration Protocol (DHCP) server. See *DHCP Settings* on page 70.
	Starting IP Address	Specify the start of the range for the pool of IP addresses in the same subnet as the router.
	Ending IP Address	Specify the end of the range for the pool of IP addresses in the same subnet as the router.
Address Reservation For more information, see *DHCP Settings* on page 70.		When you specify a reserved IP address for a computer on the LAN, that computer receives the same IP address each time it access the router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings.

DHCP Settings

By default, the router functions as a Dynamic Host Configuration Protocol (DHCP) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the router's LAN. The assigned default gateway address is the LAN address of the router. IP addresses is assigned to the attached PCs from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the router are satisfactory. Click the link to the online document *ITCP/IP Networking Basics* on page 96 for an explanation of DHCP and information about how to assign IP addresses for your network.

Use Router as DHCP Server

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the **Use Router as DHCP Server** check box on the LAN IP Setup screen. Otherwise, leave it selected.

Specify the pool of IP addresses to be assigned by filling in the **Starting IP Address** and **Ending IP Address** fields. These addresses should be part of the same IP address subnet as the router's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.254, although you might want to save part of the range for devices with fixed addresses.

The router delivers the following parameters to any LAN device that requests DHCP:

- An IP address from the range you have defined.
- Subnet mask.
- Gateway IP address is the router's LAN IP address.
- Primary DNS server, if you entered a primary DNS address in the Basic Settings screen; otherwise, the router's LAN IP address.
- Secondary DNS server, if you entered a secondary DNS address in the Basic Settings screen.
- WINS server (Windows Internet Naming Service Server) determines the IP address associated with a particular Windows computer. A WINS server records and reports a list of names and IP address of Windows PCs on its local network. If you connect to a remote network that contains a WINS server, enter the server's IP address here. This allows your PCs to browse the network using the Network Neighborhood feature of Windows.

Reserved IP Addresses

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it access the router's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

To reserve an IP address:

1. Click the **Add** button.
2. In the **IP Address** field, type the IP address to assign to the computer or server. Choose an IP address from the router's LAN subnet, such as 192.168.0.x.
3. Type the MAC address of the computer or server.

    Tip: If the computer is on your network, it is listed on the same screen for your convenience. Clicking the radio button for each entry in the attached device list fills in the fields automatically with the computer's MAC address and name.

4. Click **Apply** to enter the reserved address into the table.

Note: The reserved address will not be assigned until the next time the computer contacts the router's DHCP server. Reboot the computer or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry:

1. Click the button next to the reserved address you want to edit or delete.
2. Click **Edit** or **Delete**.

QoS Setup

QoS is an advanced feature that can be used to prioritize some Internet applications and online gaming, and to minimize the impact when the bandwidth is busy.

From the main menu, select QoS Setup to display the following screen:

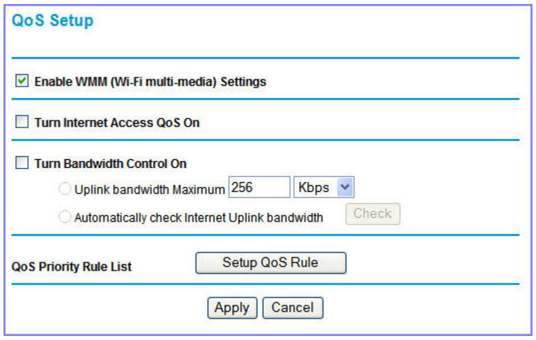
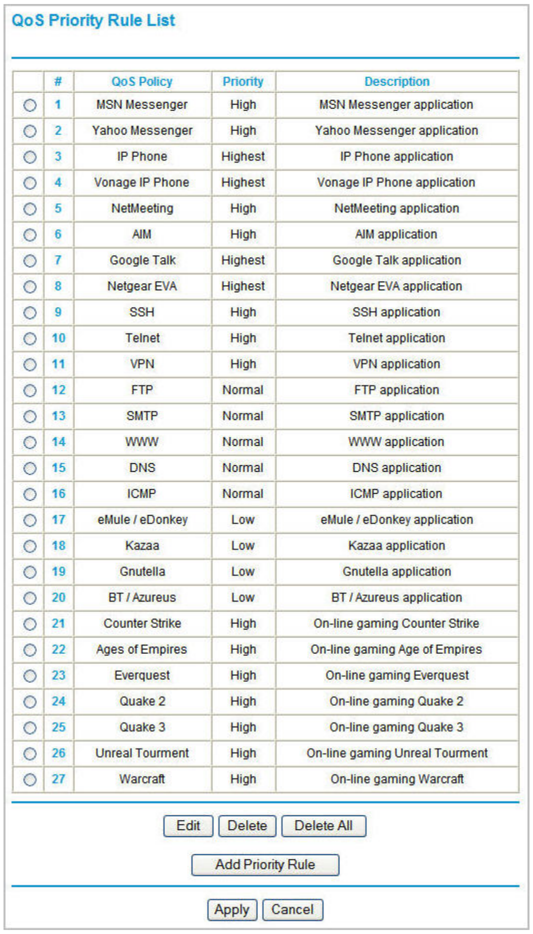


Table 6.

Field	Description
Wi-Fi Multi-media (WMM) Settings	WMM (Wireless Multimedia) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities depending on the kind of data. Time-dependent information, such as video or audio, has a higher priority than normal traffic. For WMM to function correctly, wireless clients must also support WMM.
Turn Internet Access QoS On	If you enable QoS, the QoS function works to prioritize Internet access traffic. For the applications that already exist in the drop-down list (e.g., On-line Gaming, Ethernet LAN Port, or a specified MAC address), you can modify the priority level by clicking the **Edit** button, or clicking the **Delete** button to erase the priority rule. Otherwise, you can also define the priority policy for online gaming, an application, a LAN port, or the computer's MAC address by clicking the **Add Priority Rule** button.
Bandwidth Control	To set up the total maximum uplink bandwidth, click the **Check** button to detect current uplink bandwidth that will help you to determinate the maximum bandwidth setting.

QoS Priority Rule List

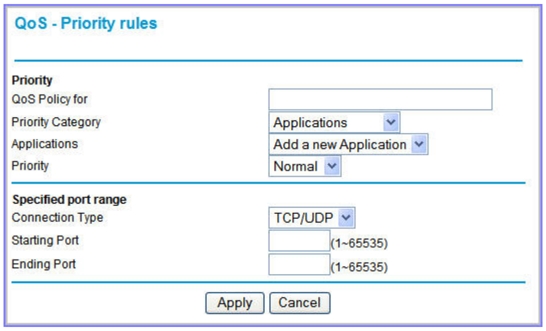
From the QoS Setup screen, click **Setup QoS Rule** to display the following screen:



	#	QoS Policy	Priority	Description
○	1	MSN Messenger	High	MSN Messenger application
○	2	Yahoo Messenger	High	Yahoo Messenger application
○	3	IP Phone	Highest	IP Phone application
○	4	Vonage IP Phone	Highest	Vonage IP Phone application
○	5	NetMeeting	High	NetMeeting application
○	6	AIM	High	AIM application
○	7	Google Talk	Highest	Google Talk application
○	8	Netgear EVA	Highest	Netgear EVA application
○	9	SSH	High	SSH application
○	10	Telnet	High	Telnet application
○	11	VPN	High	VPN application
○	12	FTP	Normal	FTP application
○	13	SMTP	Normal	SMTP application
○	14	WWW	Normal	WWW application
○	15	DNS	Normal	DNS application
○	16	ICMP	Normal	ICMP application
○	17	eMule / eDonkey	Low	eMule / eDonkey application
○	18	Kazaa	Low	Kazaa application
○	19	Gnutella	Low	Gnutella application
○	20	BT / Azureus	Low	BT / Azureus application
○	21	Counter Strike	High	On-line gaming Counter Strike
○	22	Ages of Empires	High	On-line gaming Age of Empires
○	23	Everquest	High	On-line gaming Everquest
○	24	Quake 2	High	On-line gaming Quake 2
○	25	Quake 3	High	On-line gaming Quake 3
○	26	Unreal Tourment	High	On-line gaming Unreal Tourment
○	27	Warcraft	High	On-line gaming Warcraft

QoS Priority Rules

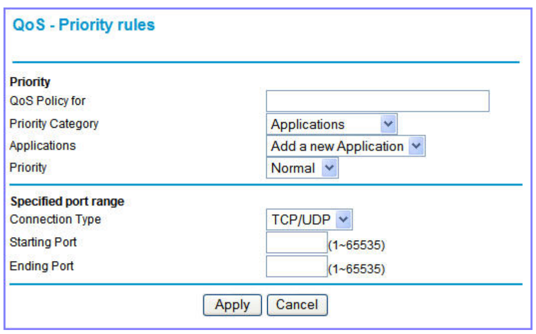
From the QoS Priority Rule List, click **Add Priority Rule** to display the following screen:



For Applications or Online Gaming

To set up the priority for an application or online gaming:

1. Select **Applications** or **On-line Gaming** from the **Priority Category** lists.



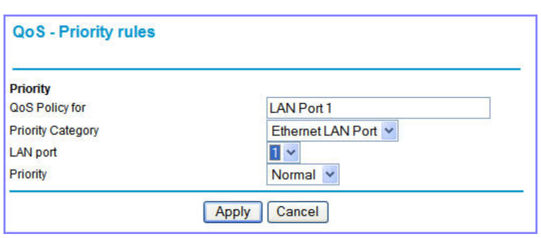


2. Select the Internet application or game for which you want to set the priority from the relevant list.
3. Select the priority level: **Highest**, **High**, **Normal**, or **Low**.
4. You can also type the name in the **QoS Policy** field for this rule if you prefer.
5. Click **Apply**.

For Ethernet LAN Ports

To set up the priority for LAN port:

1. Select **Ethernet LAN Port** from the **Priority Category** list.

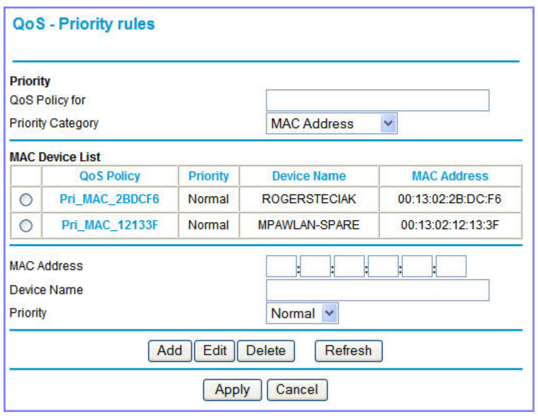


2. Select the LAN port number you plan to specify the priority level for those computers connecting on this LAN port.
3. Select the priority level: **Highest**, **High**, **Normal**, or **Low**.
4. You can also type the name in the **QoS Policy** field for this rule if you prefer.
5. Click **Apply**.

For MAC Addresses

To set up the priority for specified computer via its MAC address:

1. Select **MAC Address** from the **Priority Category** list.



2. Click the **Refresh** button to update the list of computers already connected to the router.
3. Select the entry's radio button.
4. Modify the information in the **MAC Address** and **Device Name** fields.
5. Select the priority level: **Highest**, **High**, **Normal**, or **Low**.
6. You can also type the name in the **QoS Policy** field for this rule if you prefer.
7. Click the **Edit** button.
8. Click **Apply**.

To add the priority for specified computer via its MAC address:

1. Choose **MAC Address** from the **Priority Category** list.
2. Enter the MAC address for the computer for which you are specifying the priority.
3. You can also type a name that is easy to remember in the **Device Name** fields.
4. Select the priority level: **Highest**, **High**, **Normal**, or **Low**.
5. You can also type a name in the **QoS Policy** field for this rule if you prefer.
6. Click the **Add** button.
7. Click **Apply**.

To delete a priority rule entry:

1. Select the entry's radio button of the table.
2. Click the **Delete** button.
3. Click **Apply**.

Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service to register your domain to their IP address, and forward traffic directed at your domain to your frequently changing IP address.

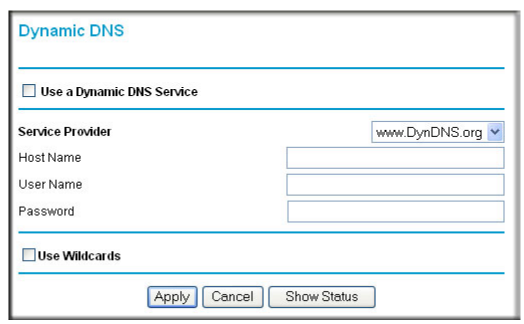
The router contains a client that can connect to a Dynamic DNS service provider. To use this feature, you must select a service provider and obtain an account with them. After you have configured your account information in the router, whenever your ISP-assigned IP address changes, your router will automatically contact your Dynamic DNS service provider, log in to your account, and register your new IP address.

WARNING!

If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the Dynamic DNS service will not work because private addresses will not be routed on the Internet.

To configure Dynamic DNS:

1. From the main menu, select **Dynamic DNS** to display the Dynamic DNS screen:



2. Access the website of one of the Dynamic DNS service providers whose names appear in the **Service Provider** drop-down list, and register for an account.

   For example, for dyndns.org, go to www.dyndns.org.
3. Select the **Use a Dynamic DNS Service** check box.
4. Select the name of your Dynamic DNS service provider.
5. Fill in the **Host Name**, **User Name**, and **Password** fields.

   The Dynamic DNS service provider might call the host name a domain name. If your URL is myName.dyndns.org, then your host name is myName. The password can be a key for your Dynamic DNS account.

   If your Dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the **Use wildcards** check box to activate this feature.

   For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.
6. Click **Apply** to save your configuration.

Using Static Routes

Static routes provide additional routing information to your router. Under normal circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You must configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

Static Route Example

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.
- Your company's network is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the router, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you must define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100.

In this example:

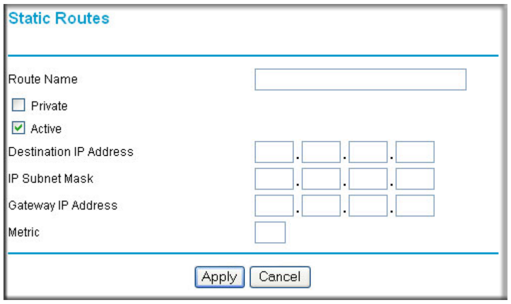
- The **Destination IP Address** and **IP Subnet Mask** fields specify that this static route applies to all 134.177.x.x addresses.
- The **Gateway IP Address** fields specify that all traffic for these addresses should be forwarded to the ISDN router at 192.168.0.100.
- In the **Metric** field, a value of 1 will work since the ISDN router is on the LAN.
  This represents the number of routers between your network and the destination. This is a direct connection, so it is set to 1.
- **Private** is selected only as a precautionary security measure in case RIP is activated.

To configure static routes:

1. From the main menu, under Advanced, select Static Routes to view the Static Routes screen.



2. Select the radio button of the static route you want to configure.
3. Click **Add** or **Edit** to display the following screen:



4. Fill in or change the fields:
   - **Route Name.** The route name is for identification purposes only.
   - **Private**. Select this check box if you want to limit access to the LAN only. The static route will not be reported in RIP.
   - **Active**. Select this check box to make this route effective.
   - **Destination IP Address**, and **IP Subnet Mask**. If the destination is a single host, type a subnet value of **255.255.255.255**.
   - **Gateway IP Address**. This must be a router on the same LAN segment as the router.
   - **Metric**. Type a number between 2 and 15. This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 2.
5. Click **Apply** to save your changes. If you added a static route, it is added to the Static Routes screen.

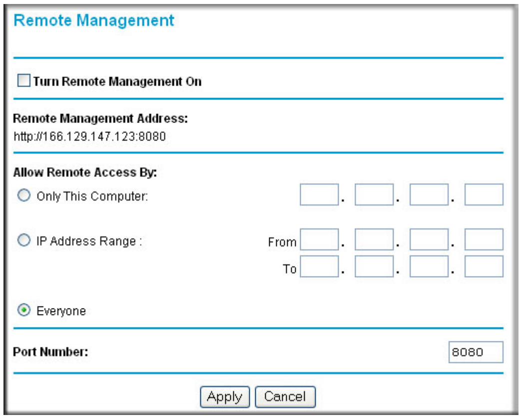
Enabling Remote Management

Using the Remote Management screen, you can allow a user or users on the Internet to configure, upgrade, and check the status of your router.

Tip: Be sure to change the router default password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper-case and lower-case), numbers, and symbols. Your password can be up to 30 characters.

To configure Remote Management

1. Log in to the router. Type **http://www.routerlogin.net** in the address field of your Internet browser. Enter **admin** for the user name and your password (or the default, **password**).
2. Under Advanced, select Remote Management:



3. Select the **Turn Remote Management On** check box.
4. Specify which external addresses will be allowed to access the router's remote management.

   For security, restrict access to as few external IP addresses as practical:

   - To allow access from any IP address on the Internet, select **Everyone**.
   - To allow access from a range of IP addresses on the Internet, select **IP Address Range**. Enter a beginning and ending IP address to define the allowed range.
   - To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that will be allowed access.
5. Specify the port number that will be used for accessing the router menu.

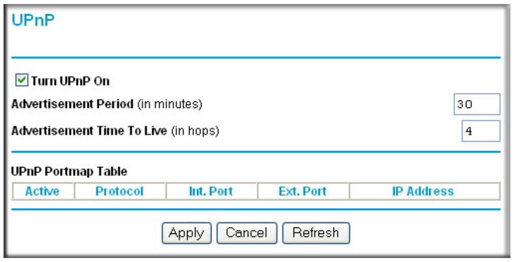
   Access normally uses the standard HTTP service port 80. For greater security, you can enter a different port number. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.
6. Click **Apply** to have your changes take effect.

   When accessing your router from the Internet, type your router WAN IP address in your Internet browser address or location field, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter: **http://134.177.0.123:8080.** Be sure to include http:// in the address.

Universal Plug and Play

Universal Plug and Play (UPnP) helps devices such as Internet appliances and computers access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

1. Select UPnP on the main menu to display the UPnP screen:

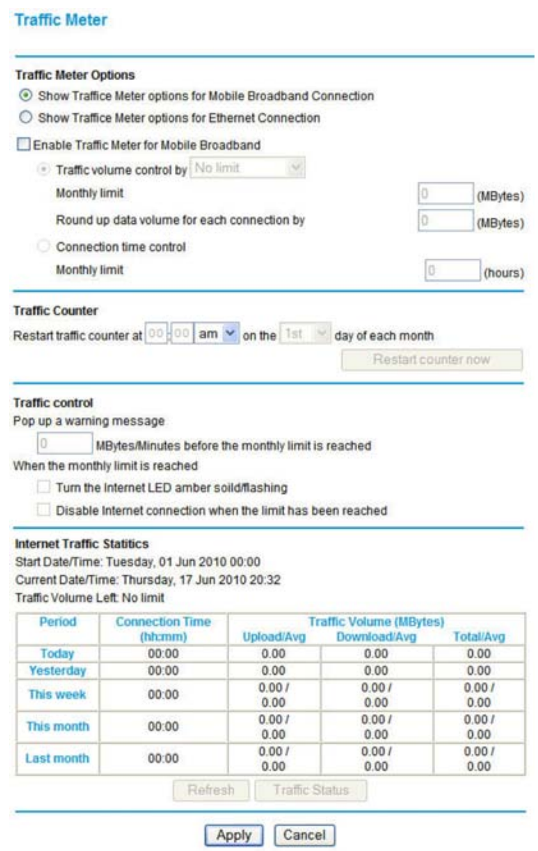


2. Fill in the settings on the UPnP screen:
   - **Turn UPnP On**. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If this feature is disabled, the router will not allow any device to automatically control the resources, such as port forwarding (mapping), of the router.
   - **Advertisement Period**. The advertisement period is how often the router advertises (broadcasts) its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations might compromise the freshness of the device status but can significantly reduce network traffic.
   - **Advertisement Time To Live**. The time to live for the advertisement is measured in hops for each UPnP packet sent. A hop is the number of steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which should be fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it might be necessary to increase this value a little.
   - **UPnP Portmap Table**. The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the router and which ports (internal and external) that device has opened.
3. To save or cancel your changes or refresh the table:
   - Click **Apply** to save the new settings to the router.
   - Click **Cancel** to disregard any unsaved changes.
   - Click **Refresh** to update the portmap table and to show the active ports that are currently opened by UPnP devices.

Traffic Meter

Traffic metering allows you to monitor the volume of Internet traffic passing through your router's Internet port. With the Traffic Meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage. You enable separate traffic meters for the mobile broadband connection and the Ethernet connection.

To monitor traffic on your router:



1. Under Advanced on the router menu, select Traffic Meter.
2. Click the appropriate **Show Traffic Meter Application for ...** radio button for the type of Internet connection (e.g., mobile broadband or Ethernet) you are setting up.
3. To enable the traffic meter, select the **Enable Traffic Meter** check box.
4. If you would like to record and restrict the volume of Internet traffic, select the **Traffic volume control by** radio button. You can select one of the following options for controlling the traffic volume:
   - **No Limit**. No restriction is applied when the traffic limit is reached.
   - **Download only**. The restriction is applied to incoming traffic only.
   - **Both Directions**. The restriction is applied to both incoming and outgoing traffic.
5. You can limit the amount of data traffic allowed per month:
   - By specifying how many Mbytes per month are allowed.
   - By specifying how many hours of traffic are allowed.
6. Set the Traffic Counter to begin at a specific time and date.
7. Set up traffic control to issue a warning message before the monthly limit of Mbytes or hours is reached. You can select one of the following to occur when the limit is attained:
   - The Internet LED flashes green or amber.
   - The Internet connection is disconnected and disabled.
8. Set up **Internet Traffic Statistics** to monitor the data traffic.
9. Click the **Traffic Status** button if you want a live update on Internet traffic status on your router.
10. Click **Apply** to save your settings.

6. Troubleshooting

6

This chapter gives information about troubleshooting your Mobile Broadband 11n Wireless Router. After each problem description, instructions are provided to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the router on?

  Go to *Basic Functioning* on page 84.

- Have I connected the router correctly?

  Go to *Basic Functioning* on page 84.

- I can't access the router's configuration with my browser.

  Go to *Troubleshooting Access to the Router Main Menu* on page 86.

- I've configured the router but I can't access the Internet.

  Go to *Troubleshooting the ISP Connection* on page 87.

- I want to clear the configuration and start over again.

  Go to *Restoring the Default Configuration and Password* on page 91.

Basic Functioning

After you turn on power to the router, the following sequence of events should occur:

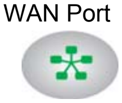
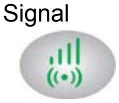
1. When power is first applied, verify that the Power LED is on.
2. After approximately 10 seconds, verify that:
   a. The Power LED is still solid green. An amber light indicates the unit has failed its power-on self-test (POST).
   b. The Internet LED is lit.
   c. The Wi-Fi radio LED is lit. The Wi-Fi radio is on by default.
   d. The Ethernet LAN port LED is lit when any local ports are connected.

      If a LAN port's LED is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED is amber.

   e. The Ethernet WAN port LED is lit when the router is connected to a wired modem.
   f. The Signal LED is lit when the router has detected a mobile broadband signal.
      - A blue LED indicates excellent coverage.
      - A green LED indicates good coverage.
      - An amber LED indicates marginal coverage.

If any of these conditions does not occur, refer to the following table.

LED		Action
Power	Power LED is off.	• Make sure the power cord is correctly connected to your router, and that the power supply adapter is correctly connected to a functioning power outlet. • Check that you are using the power adapter supplied by NETGEAR for this product. • If the error persists, you might have a hardware problem and should contact Technical Support.
	Power LED is amber.	There is a fault within the router. Try to clear the fault as follows: • Cycle the power to see if the router recovers. • Clear the router's configuration to factory defaults. This sets the router's IP address to 192.168.0.1. This procedure is explained in *Restoring the Default Configuration and Password* on page 91. If the error persists, you might have a hardware problem and should contact Technical Support.

LED		Action
Internet Port 	Internet LED is off.	Be sure the SIM card you received is in the router. SIM cards from other devices will not function in the router, and the this SIM card will not function in other devices.
	Internet LED is amber.	The router cannot connect to the Internet. Check the Internet connection option being used. • For the mobile broadband connection option, check the Signal LED. • For the Ethernet connection option, check the WAN LED.
	Internet LED is blinking amber and green.	The Traffic Meter feature is enabled, and the limit set has been reached.
Wi-Fi 	Wi-Fi LED is off.	The Wi-Fi radio has been turned off. If you want a Wi-Fi connection with the router, push the Wi-Fi button to turn the Wi-Fi radio back on.
	Wi-Fi LED is not blinking.	If this LED does not blink when you are attempting to send data over the Wi-Fi link, log in to the router menu using the Ethernet LAN connection and check your router's wireless (Wi-Fi) configuration.
LAN Ports 	LAN LED is off.	If this LED does not light when an Ethernet connection is made, check the following: • Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation. • Make sure that power is turned on to the connected hub or workstation.
WAN Port 	WAN LED is off.	If this LED does not light when an Ethernet connection is made using the Ethernet connection option, check the following: • Make sure that the Ethernet cable connections are secure at the router and at the modem. • Make sure that power is turned on to the modem.
2G/3G 	2G/3G LED is off.	The router cannot tell if the mobile broadband connection uses 2G or 3G signals.
Signal 	Signal LED is off or amber.	If this LED does not light when the Mobile Broadband connection option is used, check the following: • Check with your ISP to ensure that there is good coverage in the area. • Ensurethat your mobile broadband account is active. • Ensure that the SIM card is inserted correclty into the router. • Locate the router near the window or other area of the building. Make sure that the Signal LED is lit, indicating there is mobile broadband coverage with the router. • Log in to the router menu and check the Internet configuration. Check that the user name, password, and APN with ISP are set correctly. If you use a PIN to connect to the Internet, make sure it is entered correctly.

Troubleshooting Access to the Router Main Menu

If you are unable to access the router main menu from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router as described in the previous section.
- Make sure your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range of 192.168.0.2 to 192.168.0.254. See the online document you can access from *ITCP/IP Networking Basics* in Appendix A to find your computer's IP address.

Note: If your computer's IP address is shown as 169.254.x.x:
Recent versions of Windows and MacOS generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router, and reboot your computer.

- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in *Restoring the Default Configuration and Password* on page 91.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when entering this information.

If the router does not save changes you have made in the Web Man agement Interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the Web browser. The changes might have occurred, but the Web browser might be caching the old configuration.

Troubleshooting the ISP Connection

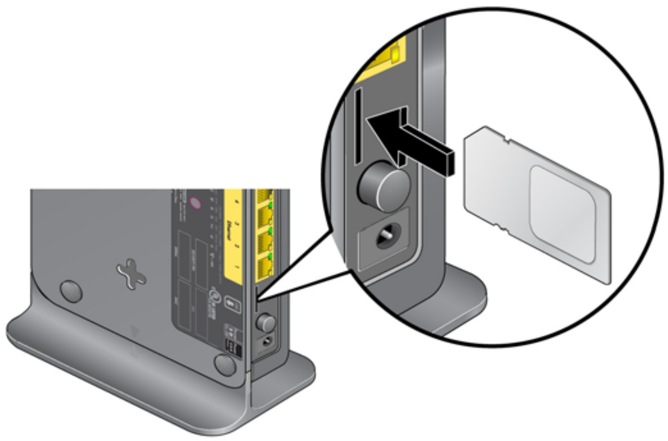
Check these possible sources of trouble if you are having difficulty connecting to or browsing the Internet.

Connecting to the Internet

If unable to connect to Internet, check the following:

1. The Internet account is active.

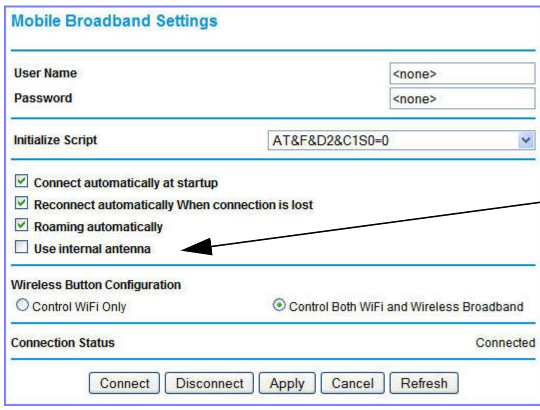
   If your ISP has provided you with a SIM card and you haven't inserted it into the SIM card slot on the back of the router yet, do so now.



2. Wireless broadband coverage is available where the unit is located.
3. Access the router main menu to verify that the broadband settings are correct. Check with your ISP if you are unsure.
4. Check the location of the router.
   - **a.** Move the router closer to a window for better access to the Internet signal.
     - A blue Signal LED indicates excellent coverage.
     - A green Signal LED indicates good coverage.
     - An amber Signal LED indicates marginal coverage.
     - An unlighted Signal LED indicates no coverage.
   - **b.** Maintain recommended minimum distances between NETGEAR equipment and household appliances to reduce interference (see *Regulatory Compliance Information* on page 97).

5. Using an external antenna for improved signal strength:





a. Install an external antenna. (The external antenna is an optional accessory that you can purchase.)

b. Clear the **Use Internal Antenna** check box on the Mobile Broadband Settings screen and then click **Apply**.

c. Click **Connect** to connect to the Internet.

Troubleshooting Internet Browsing

If your router can obtain an IP address but your computer is unable to load any Web pages from the Internet:

- The traffic meter is enabled, and the limit might have been reached.

  By configuring the traffic meter not to block, you can resume Internet access. If you have an usage limit, your ISP might charge you for the overage.

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the router’s configuration, reboot your computer and verify the DNS address as described in the article you can access from *ITCP/IP Networking Basics* in Appendix A. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer might not have the router configured as its TCP/IP router.

  If your computer obtains its information from the router by DHCP, reboot the computer, and verify the router address as described in the online document you can access from *ITCP/IP Networking Basics* in Appendix A.

Troubleshooting a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshoot a TCP/IP network by using the ping utility in your computer.

Testing the LAN Path to Your Router

You can ping the router from your PC to verify that the LAN path to your router is set up correctly.

To ping the router from a PC running Windows 95 or later:

1. From the Windows toolbar, click the Start button, and select Run.
2. In the field provided, type **ping** followed by the IP address of the router, as in this example:

   ping 192.168.0.1
3. Click **OK**.

   You should see a message like this one:

   Pinging <IP address> with 32 bytes of data

   If the path is working, you see this message:

   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx

   If the path is not working, you see this message:

   Request timed out

   If the path is not working correctly, you could have one of the following problems:

   - Wrong physical connections
     - Make sure that the LAN port LED is on. If the LED is off, follow the instructions in *Connecting to the Internet* on page 87.
     - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.
   - Wrong network configuration
     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
     - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device.

1. From the Windows toolbar, click the Start button, and select Run.
2. In the Windows Run window, type:

   `ping -n 10` *IP address*

   where *IP address* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your router listed as the default router. If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default router as described in the online document you can access from *Preparing Your Network* in Appendix A.
- Make sure that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the account name in the Basic Settings screen.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing only traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your router to clone or spoof the MAC address from the authorized PC. See the *Mobile Broadband 11n Wireless Router MBR1210 Installation Guide*.

Problems with Date and Time

The email screen displays the current date and time of day. The Mobile Broadband 11n Wireless Router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date shown is January 1, 2000.
  Cause: The router has not yet successfully reached a network time server. Check that your Internet access settings are configured correctly. If you have just completed configuring the router, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour.
  Cause: The router does not automatically sense daylight savings time. On the E-mail screen, select or clear the **Adjust for Daylight Savings Time** check box.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router's admin password to **password** and the IP address to **192.168.0.1**. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase feature (see *Erasing the Configuration* on page 54).
- Press the Restore Factory Settings button on the bottom of the router for 6 seconds. Use this method for cases when the administration password or IP address is not known.

The factory default settings are shown in *Factory Default Settings* in Appendix A.

A. Supplemental Information

A

This appendix provides the following information:

- **Factory Default Settings**
- **Technical Specifications**
- **Related Documents**

Factory Default Settings

Use the Restore Factory Settings button located on the bottom of your router to reset all settings to their original factory default settings. This is called a hard reset. To perform a hard reset, push and hold the Restore Factory Settings button for 6 seconds. Your router will return to the factory configuration settings that are shown in the following table.

Feature		Default Behavior
Router login	User login URL	http://www.routerlogin.net *or* http://www.routerlogin.com
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Internet Connection	WAN MAC address	Use default address
	WAN MTU size	1500
	Port speed	AutoSense
Local network (LAN)	LAN IP	192.168.0.1
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	None
	DHCP server	Enabled
	DHCP starting IP address	192.168.0.2
	DHCP ending IP address	192.168.0.254
	DMZ	Disabled
	Time zone	EST for North America
	Daylight saving time adjustment	Disabled
Firewall	Inbound communication from the Internet	Disabled (except traffic on port 80, the HTTP port)
	Outbound communication to the Internet)	Enabled (all)
	Source MAC filtering	Disabled

Feature (Continued)		**Default Behavior (Continued)**
Mobile Broadband	Internet Service Provider:	Bell Mobility
	APN:	inet.bell.ca
	Access Number:	*99#
	PDP Type:	IP
	Username:	none required
WiFi	Wireless communication	Enabled
	SSID name	See label on the bottom of router
	Security	WPA-PSK/WPA2-PSK mixed mode
	Broadcast SSID	Enabled
	Transmission speed	Auto (maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.)
	Country/Region	Canada
	RF channel	Auto
	Operating mode	Up to 145 Mbps
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Open system
	Wireless Card Access List	All wireless stations allowed

Technical Specifications

Technical Specifications	
Network Protocol and Standards Compatibility	TCP/IP, DHCP
Power adapter	• North America: 120V AC, 60 Hz, input • 12V DC @ 1.5A output
Physical specifications	• Dimensions: 6.8 in. x 5.03 in. x 1.28 in. (173 mm x 128 mm x 33 mm) • Weight: 0.65 lbs. without the stand (0.29 kg)
Environmental Specifications	• Operating temperature: 0° to 40° C (32º to 104º F) • Operating humidity: 90% maximum relative humidity, noncondensing
Electromagnetic Emissions	FCC Part 15 Class B; IC; EN 55 022 (CISPR 22), Class B
Interface Specifications	• LAN: 10BASE-T or 100BASE-Tx, RJ-45 • WAN: 10BASE-T or 100BASE-TX, RJ-45
Antenna Connection (Optional)	• R-TNC connector

Related Documents

The table below provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Using Microsoft Vista and Windows XP to Manage Wireless Network Connections	*http://documentation.netgear.com/reference/enu/winzerocfg/index.htm*
ITCP/IP Networking Basics Wireless Networking Basics	*http://documentation.netgear.com/reference/enu/tcpip/index.htm* *http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing Your Network	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Virtual Private Networking Basics	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

Notification of Compliance

NETGEAR Wireless Routers, Gateways, AP's

B

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

Note: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the Routeur sans fil MBR1210 11n à haut débit mobile complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus, Routeur sans fil MBR1210 11n à haut débit mobile, does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Europe – EU Declaration of Conformity

Marking with the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC).

This equipment meets the following conformance standards:

- EN300 328 (2.4Ghz), EN301 489-17, EN301 893 (5Ghz), EN60950-1
- This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.
- In Italy, the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.
- This device may not be used for setting up outdoor radio links in France, and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information contact the national spectrum authority in France.

  For complete DoC, visit the NETGEAR EU Declarations of Conformity website at::
  http://kb.netgear.com/app/answers/detail/a_id/11621/

Table 1. EDOC in Languages of the European Community

Language	Statement
Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

Table 1. EDOC in Languages of the European Community

Language	Statement
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.

Table 1. EDOC in Languages of the European Community

Language	Statement
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

Interference Reduction Table

The table below shows the Recommended Minimum Distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Table 2. Interference Reduction Table

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby Monitor - Analog	20 feet / 6 meters
Baby Monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters

Index

Soutien technique

Nous vous remercions d'avoir choisi NETGEAR. Pour enregistrer votre produit, vous procurer les mises à jour les plus récentes ou obtenir un soutien technique en ligne, rendez-vous sur le site *http://support.netgear.com*.

Téléphone (Canada et États-Unis seulement) : 1-888-NETGEAR

Téléphone (autres pays) : reportez-vous à la carte d'information sur le soutien technique.

Marques commerciales

NETGEAR, le logo NETGEAR, ReadyNAS, ProSafe, Smart Wizard, Auto Uplink, X-RAID2 et NeoTV sont des marques de commerce ou des marques déposées de NETGEAR, Inc. Microsoft, Windows, Windows NT et Vista sont des marques déposées de Microsoft Corporation. Les autres marques et noms de produits sont des marques de commerce ou des marques déposées de leurs détenteurs respectifs.

Conditions

Afin d'améliorer la conception, les fonctions opérationnelles ou la fiabilité de l'équipement, NETGEAR se réserve le droit de modifier sans préavis les produits décrits dans ce document. NETGEAR décline toute responsabilité quant aux conséquences de l'utilisation des produits ou des configurations de circuits décrits dans ce document.

Historique des versions

Numéro de publication	Version	Date de publication	Commentaires
202-10734-03	v1.0	October 2010	Première publication

Table des matières

FRANÇAIS CANADIEN

Chapitre 1 Connexion à Internet

Chapitre 2 Configuration du réseau sans fil

Chapitre 3 Filtrage de contenu

Chapitre 4 Gestion de votre réseau

Chapitre 5 Avancé

Chapitre 6 Dépannage

1. Connexion à Internet

Ce chapitre explique comment configurer la connexion Internet du Routeur sans fil MBR1210 11n à haut débit mobile.

- **Caractéristiques matérielles**
- **Connexion à votre routeur**
- **Accès à l'assistant de configuration après l'installation**
- **Configuration manuelle de vos paramètres Internet**

Remarque : Pour en savoir plus sur l'installation, consultez le *Mobile Broadband 11n Wireless Router MBR1210 Installation Guide.*

Caractéristiques matérielles

Cette section présente les caractéristiques physiques de votre Mobile Broadband 11n Wireless Router.

Support du routeur

Comme le Mobile Broadband 11n Wireless Router s'utilise uniquement à la verticale, servez-vous du support pour placer le router dans cette position.

1. Insérez les pattes du support dans les fentes situées sous le routeur.
2. Placez le routeur près d'une prise d'adaptateur secteur CA, à un endroit d'où vous pourrez connecter les câbles nécessaires pour le réseau domestique.

   Vous devez également vous assurer que le routeur se trouve à un endroit où vous pourrez recevoir un signal haut débit mobile puissant à l'intérieur de la maison, si vous prévoyez vous connecter à Internet avec une connexion haut débit mobile.

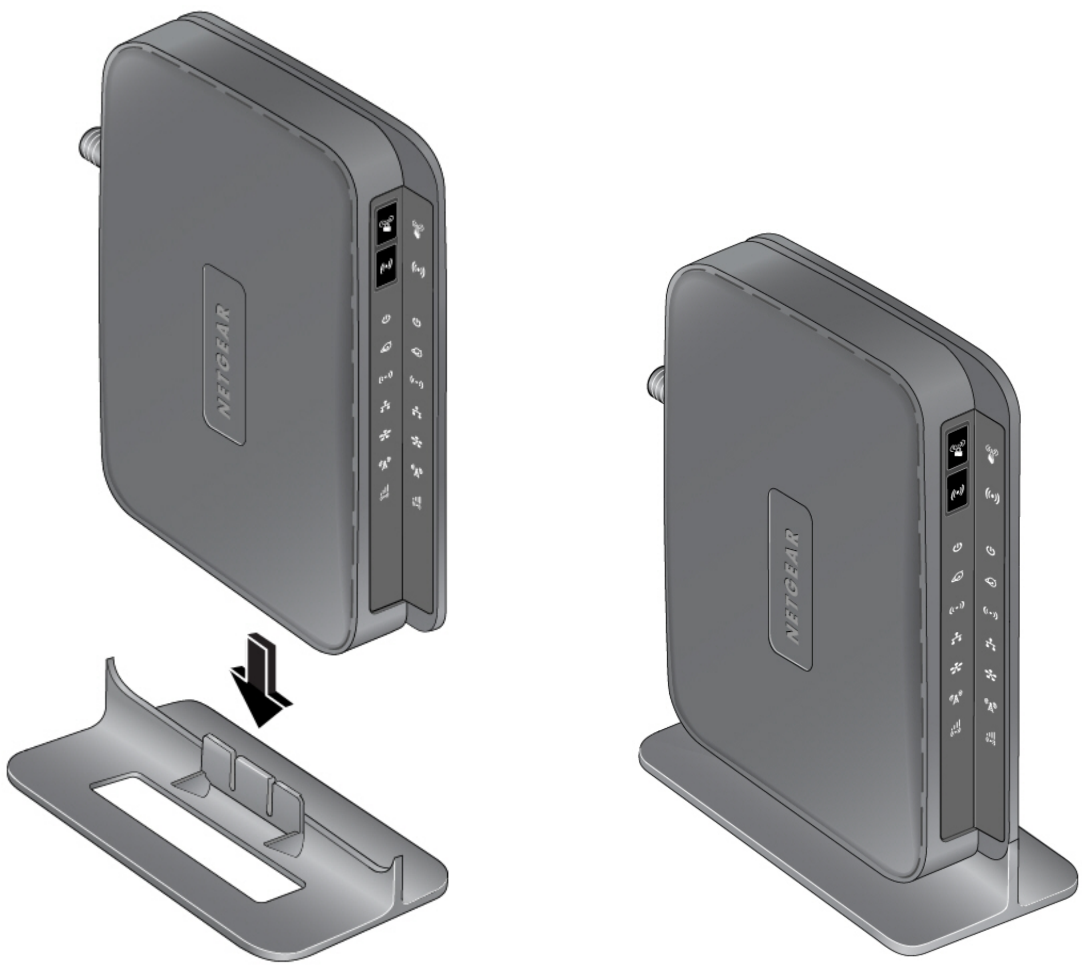


Figure 1.

Panneau avant du routeur

Le panneau avant du router comporte des boutons de commande et des voyants d'état. Les voyants vous permettent de vérifier l'état de l'appareil et les connexions en cours.

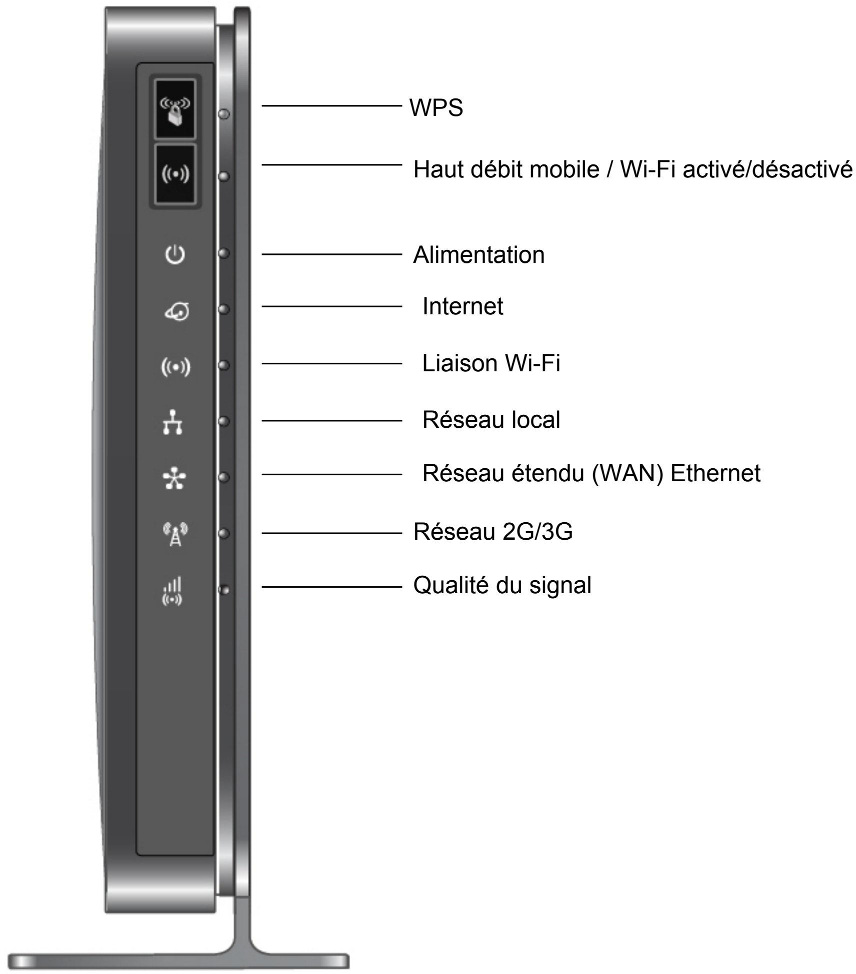


Figure 2.

Le *Tableau 20* présente une description de tous les voyants et boutons situés sur le panneau avant du router.

Tableau 1. Description des voyants

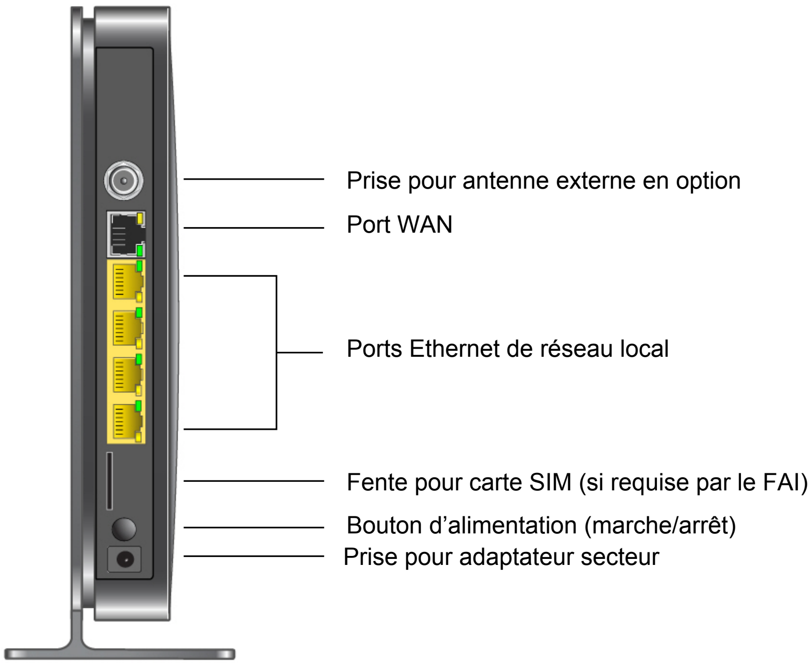
Voyant	Activité	Description
WPS 	Appuyez sur le bouton WPS pour tenter de connecter le router à d'autres périphériques WPS. Le délai de connexion est de deux minutes. Pour en savoir plus sur cette fonction, consultez la section *Utilisation de la fonctionnalité « Appuyez : vous êtes connecté » (WPS) pour configurer votre réseau sans fil* à la page 133.	
Liaison Wi-Fi 	Ce bouton permet de contrôler seulement la liaison radio Wi-Fi ou bien la liaison radio Wi-Fi et la liaison radio haut débit mobile. Utilisez l'interface pour sélectionner les options désirées. La liaison Wi-Fi est activée par défaut.	

Tableau 1. Description des voyants

Voyant	Activité	Description
Alimentation 	Vert continu	Le routeur est sous tension et fonctionne normalement.
	Orange continu	Le routeur effectue un test d'autodiagnostic.
	Éteint	Le routeur est hors tension.
Port Internet 	Vert continu	Une session Internet est en cours.
	Orange continu	La limite de trafic est atteinte et le trafic est bloqué.
	Vert clignotant	Des données sont transmises par connexion Internet.
	Orange clignotant	La limite de trafic est atteinte, mais le trafic n'est pas bloqué.
	Clignotant vert et orange	Basculement du WAN à la connexion haut débit mobile.
	Éteint	Aucune connexion Internet détectée.
Liaison Wi-Fi 	Bleu continu	Le port Wi-Fi local est initialisé.
	Bleu clignotant	Des données sont reçues ou transmises par liaison Wi-Fi.
	Éteint	Le point d'accès sans fil est désactivé.
Ports de réseau local 	Vert continu	Des liaisons filaires avec des ordinateurs ont été détectées dans les ports Ethernet locaux.
	Clignotant	Les données sont en cours de transmission ou de réception.
	Éteint	Aucune liaison n'a été détectée sur ces ports.
Port WAN 	Vert continu	Liaison active détectée sur le port Ethernet de réseau étendu.
	Clignotant	Les données sont en cours de transmission ou de réception.
	Éteint	Aucune liaison n'a été détectée sur ces ports.
Réseau 2G/3G 	Bleu continu	Indique que le routeur bénéficie d'une couverture 3G+.
	Vert continu	Indique que le routeur bénéficie d'une couverture 2G.
	Éteint	Aucune couverture n'est détectée.
Qualité du signal 	Bleu continu	Excellente couverture détectée.
	Vert continu	Bonne couverture détectée.
	Orange continu	Couverture partielle détectée.
	Éteint	Aucune couverture détectée.
Réinitialisation des paramètres d'usine 	Repérez le petit trou cerclé de rouge à l'arrière du routeur. Insérez l'extrémité d'un trombone dans le trou et appuyez pendant six secondes. Lorsque vous relâchez le bouton de réinitialisation, le voyant clignote brièvement. Une fois que vous avez enfoncé le bouton pendant plus de six secondes, le voyant clignote en orange puis il devient vert lorsque le routeur a réinitialisé les paramètres par défaut. Consultez la section	

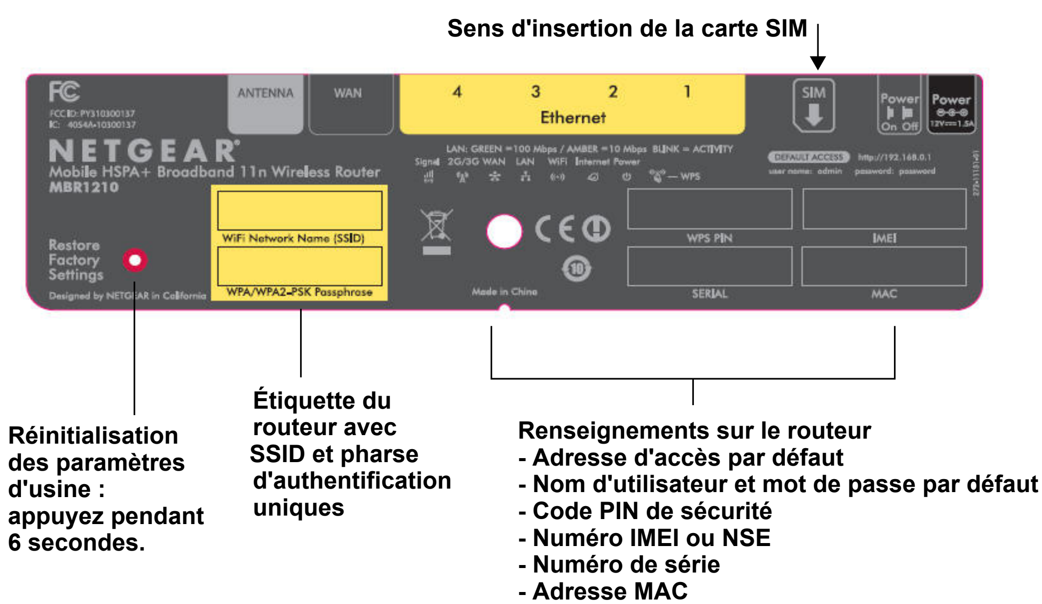
Panneau arrière du routeur

Le panneau arrière du router comporte des ports de connexion.



Étiquette du routeur

L'étiquette située à l'arrière du router mentionne son adresse MAC, son numéro de série, le code PIN de sécurité, le numéro IMEI ou NSE et les renseignements de connexion par défaut. Cette étiquette comporte également le numéro SSID et la phrase d'authentification spécifiques à chaque routeur.



Connexion à votre routeur

La première fois que vous connectez votre router durant l'installation, un assistant de configuration s'affiche. Pour savoir comment utiliser l'assistant de configuration afin de régler les paramètres de connexion Internet et de votre réseau sans fil, consultez le *Mobile Broadband 11n Wireless Router MBR1210 Installation Guide*.

Après la configuration initiale, vous pouvez utiliser votre navigateur Web pour vous connecter au router et afficher ou modifier ses paramètres. Le menu principal du router contient également des liens vers la base de connaissances et vers des documents.

Remarque : Votre ordinateur doit être configuré pour utiliser le protocole DHCP. Pour savoir comment configurer le protocole DHCP, consultez la documentation fournie avec l'ordinateur ou suivez le lien vers la documentation en ligne dans la section *Préparer votre réseau* à l'annexe A.

Une fois la connexion établie, si vous ne cliquez pas avant sur **Déconnexion**, le router coupe automatiquement la connexion après cinq minutes d'inactivité.

Pour vous connecter au router:

1. Tapez **http://www.routerlogin.net** dans le champ d'adresse du navigateur, puis appuyez sur Entrée pour accéder à la fenêtre de connexion.



2. Tapez **admin** pour le nom d'utilisateur et le mot de passe (ou la valeur par défaut **password**).

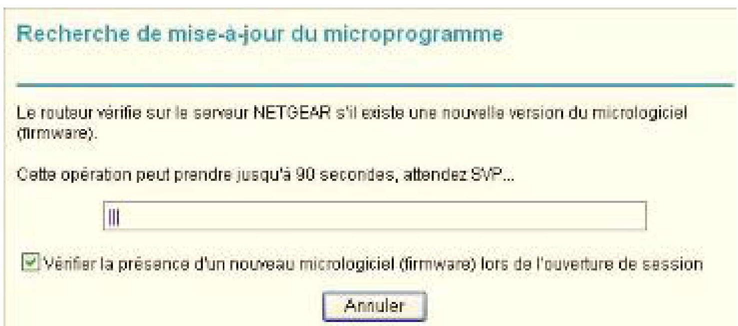
   Pour savoir comment modifier le mot de passe, consultez la section *Modification du mot de passe prédéfini* à la page 156.

Remarque : Si vous avez oublié votre mot de passe, vous pouvez réinitialiser le router à ses paramètres d'usine, ce qui rétablira le mot de passe par défaut. Consultez la section *Paramètres par défaut d'usine* à la page 194.

---

3. Si le routeur n'a pas été configuré, l'écran de l'assistant de configuration s'affiche. Une fois que le routeur a été configuré, vous accédez à l'un des écrans suivants :
   - **Écran Recherche de mise à jour du microprogramme**. Après la configuration initiale, vous accédez à l'écran Recherche de mise à jour du microprogramme, sauf si la case à cocher suivante n'est pas sélectionnée : **Vérifier la présence d'un nouveau micrologiciel (firmware) lors de l'ouverture de session**.

Remarque : Vous pouvez désactiver cette fonction de vérification et de mise à jour automatique pour les connexions subséquentes, en décochant la case **Vérifier la présence d'un nouveau micrologiciel (firmware) lors de l'ouverture de session**. NETGEAR recommande toutefois de laisser cette fonction active pour vous assurer que le routeur dispose de la toute dernière version de micrologiciel.



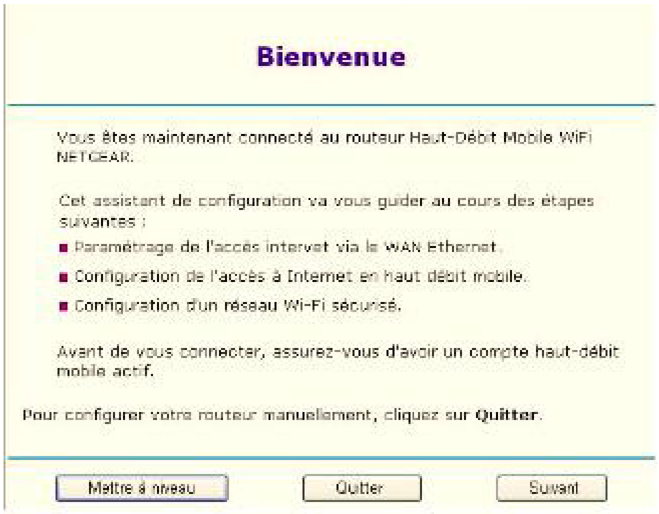
   - **Écran Statut du routeur**. L'écran Statut du routeur présente l'état de connexion actuel du routeur. Consultez la section *Statut du routeur* à la page 149.

4. Vous pouvez employer diverses méthodes pour configurer votre routeur.
   - Sélectionnez Assistant de configuration **dans le menu du routeur pour configurer votre connexion Internet et votre réseau sans fil**. Consultez la section *Accès à l'assistant de configuration après l'installation* à la page 115.
   - Vous pouvez configurer manuellement les paramètres du routeur. Consultez la section *Configuration manuelle de vos paramètres Internet* à la page 116.

Accès à l'assistant de configuration après l'installation

1. Connectez-vous au routeur en suivant les indications fournies dans la section *Connexion à votre routeur* à la page 113.

   L'assistant de configuration s'ouvre.



2. Cliquez sur **Next** (Suivant).

   L'assistant de configuration vous invite à définir les paramètres de connexion Internet ainsi que les paramètres de réseau sans fil, de la manière décrite dans le *Mobile Broadband 11n Wireless Router MBR1210 Installation Guide*.

   a. Sélectionnez votre mode de connexion Internet :
      - Use Ethernet first and if fail use mobile broadband connection (Utiliser d'abord la connexion Ethernet puis, en cas d'échec, la connexion haut débit mobile)
      - Toujours utiliser la connexion haut débit mobile
      - Always use Ethernet connection (Toujours utiliser la connexion Ethernet)



   b. Cliquez sur **Next** (Suivant).

   c. Sélectionnez une valeur dans les champs **Pays** et **Fournisseur d’accès Internet**.

   d. Cliquez sur **Done** (Terminé).

Configuration manuelle de vos paramètres Internet

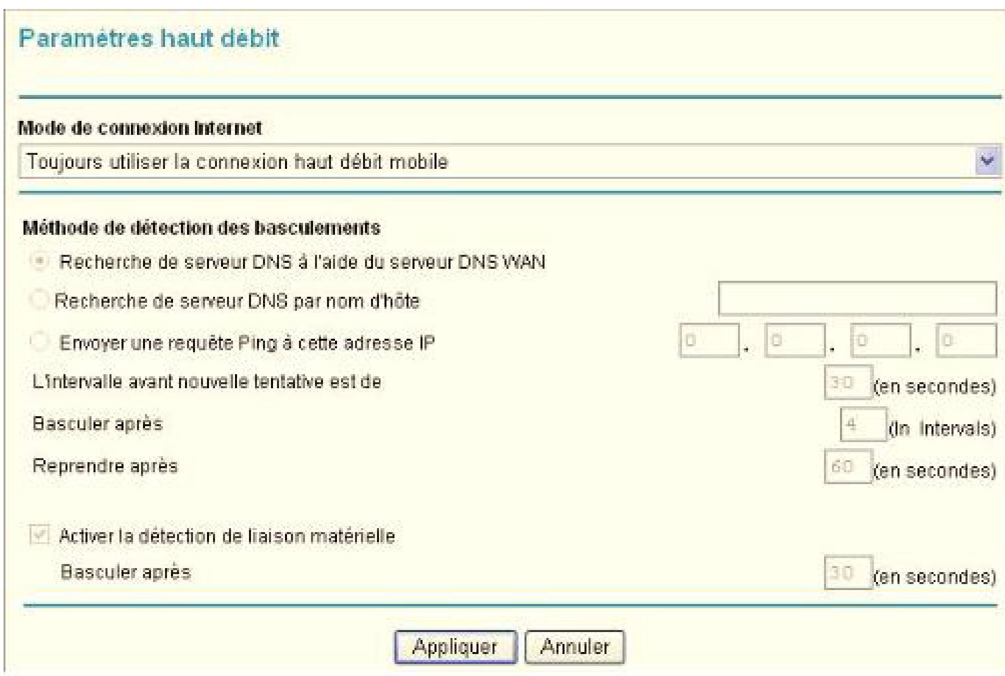
Pour pouvoir vous connecter au réseau, vous devez disposer d'un compte de service haut débit actif. Communiquez avec votre FAI pour obtenir votre nom d'utilisateur, votre mot de passe et le nom du réseau. Vous devez également configurer une partie ou l'ensemble des paramètres décrits dans les sections qui suivent, selon le mode de connexion Internet que vous avez choisi :

- *Paramètres de connexion haut débit* à la page 116.
- *Paramètres haut débit mobile* à la page 118 (non requis si vous utilisez la connexion Ethernet seulement).
- *Paramètres haut débit Ethernet* à la page 120 (non requis si vous utilisez la connexion haut débit mobile seulement).

Paramètres de connexion haut débit

Pour configurer manuellement vos paramètres de connexion Internet haut débit

1. Connectez-vous au routeur en suivant les indications fournies dans la section *Connexion à votre routeur* à la page 113.
2. Dans le menu principal, sélectionnez Paramètres haut débit.



3. Définissez les paramètres requis en fonction de votre connexion Internet. Les champs de cet écran sont décrits dans le *Tableau 21*.
4. Voici les boutons disponibles :
   - **Appliquer**. Permet d'appliquer les modifications que vous avez apportées.
   - **Annuler**. Permet de rejeter les modifications en cours.

Tableau 2. Paramètres de connexion Internet

Champs et cases à cocher	Description
Mode de connexion Internet	Les choix offerts sont : • Always use an Ethernet connection (Toujours utiliser la connexion Ethernet) (valeur par défaut) • Use Ethernet first and if it fails use mobile broadband connection (Utiliser d'abord la connexion Ethernet puis, en cas d'échec, la connexion haut débit mobile) • Toujours utiliser la connexion haut débit mobile
Méthode de détection des basculements[1]	Sélectionnez la méthode de détection des basculements et entrez les renseignements connexes : • Recherche de serveur DNS à l'aide du serveur DNS WAN • Recherche de serveur DNS par nom d'hôte • Envoyer une requête Ping à cette adresse IP
L'intervalle avant nouvelle tentative est de[1]	Entrez le délai entre chaque essai.
Basculer après[1]	Indiquez le nombre de tentatives à effectuer avant le basculement.
Reprendre après[1]	Indiquez le délai d'attente de stabilisation de la liaison primaire avant la reprise.
Activer la détection de liaison matérielle	Indiquez à quel moment basculer lorsque la liaison Ethernet est rompue. Cette option est indépendante des méthodes de détection DNS ou Ping.

*1 Ce champ est disponible uniquement si le mode de connexion Internet choisi est **Use Ethernet first and if fail use 3G mobile connection** (Utiliser d'abord la connexion Ethernet puis, en cas d'échec, la connexion 3G mobile).*

Paramètres haut débit mobile

Pour configurer manuellement vos paramètres de connexion haut débit mobile

1. Connectez-vous au routeur en suivant les indications fournies dans la section *Connexion à votre routeur* à la page 113.
2. Dans le menu principal, sélectionnez Paramètres haut débit mobile.



3. Définissez les paramètres requis en fonction de votre connexion Internet. Les champs de cet écran sont décrits dans le *Tableau 22*.
4. Voici les boutons disponibles :
   - **Connecter**. Permet d'établir manuellement la connexion au réseau.
   - **Déconnecter**. Permet de se déconnecter du réseau actuel.
   - **Appliquer**. Permet d'appliquer les modifications que vous avez apportées.
   - **Annuler**. Permet de rejeter les modifications en cours.
   - **Actualiser**. Permet de mettre à jour l'état de la connexion.

Tableau 3. Paramètres

Champs et cases à cocher	Description
Identifiant	Nom d'utilisateur pour la connexion au compte Internet.
Mot de passe	Mot de passe d'authentification pour la connexion au compte Internet.
Pays	Sélectionnez votre pays dans la liste déroulante.
Fournisseur d'accès Internet	Sélectionnez votre fournisseur de services Internet dans la liste déroulante.
Numéro d'accès	Numéro de téléphone du site distant.
Code PIN	Numéro d'identification de la carte SIM, s'il y a lieu.
Nom du point d'accès 3G	Nom du point d'accès.
Type de PDP	Sélectionnez le type de protocole de transmission des paquets de données : • **IP** • **PDP-IP** • **PPP** • **PPP-IP**
Connexion automatique au démarrage	Lorsque cette case est cochée, le modem établit automatiquement la connexion réseau au démarrage. Cette option doit être sélectionnée une fois que les renseignements de connexion ont été entrés.
Reconnexion automatique en cas de perte de connexion	Lorsque cette case est cochée, le modem tente de se reconnecter au réseau chaque fois que la connexion est rompue. Dans des situations normales, cette case devrait être cochée.
Itinérance automatique	Lorsque cette case est cochée, l'appareil peut rechercher n'importe quel opérateur disponible en itinérance; des frais d'itinérance pourraient s'appliquer.
Utiliser l'antenne interne	Lorsque cette case est cochée, le routeur utilise l'antenne interne au lieu de l'antenne externe.
Configuration du bouton sans fil	Sélectionnez l'option voulue pour déterminer le fonctionnement du bouton WPS sur le panneau avant de l'appareil. • **Contrôler le Wi-Fi uniquement** : Le bouton permet d'activer ou de désactiver la liaison Wi-Fi. Si la liaison Wi-Fi est activée, le fait d'appuyer sur le bouton la désactive. Vous pouvez appuyer de nouveau pour réactiver la liaison Wi-Fi. Cette fonction est disponible uniquement si la fonction Wi-Fi est activée. Elle n'a aucune incidence sur la fonction de connexion haut débit sans fil. • **Contrôler le Wi-Fi et le haut débit sans fil** : Le bouton permet d'activer ou de désactiver simultanément la liaison Wi-Fi et la connexion haut débit sans fil. Si la liaison Wi-Fi est activée, le fait d'appuyer sur le bouton la désactive. De plus, la connexion haut débit sans fil est également désactivée. Si vous appuyez de nouveau sur le bouton, la liaison Wi-Fi est réactivée et le routeur tente de rétablir la connexion haut débit sans fil. Selon la couverture disponible, il se peut que la connexion haut débit sans fil ne puisse pas être établie.
Statut de la connexion	Indique l'état actuel du port WAN.

Paramètres haut débit Ethernet

Pour configurer manuellement vos paramètres de connexion haut débit Ethernet

1. Connectez-vous au routeur en suivant les indications fournies dans la section *Connexion à votre routeur* à la page 113.
2. Dans le menu principal, sélectionnez Paramètres haut débit Ethernet.

   La question suivante est affichée au haut de l'écran :

   Sélectionnez une option selon le type de compte fourni par votre FAI.

   - Si vous devez entrer vos données d'identification chaque fois que vous vous connectez à Internet, ou si vous avez un compte PPPoE avec votre FAI, sélectionnez **Oui**.
   - Dans le cas contraire, sélectionnez **Non**.

   Remplissez ensuite les champs appropriés.

   Pour en savoir plus, consultez :

   étape a, Identifiant requis à la page 121

   ou

   étape b, Identifiant non requis à la page 123.

Remarque : Si vous avez installé une application PPP, comme WinPoET (d'Earthlink) ou Enternet (de PacBell), alors vous avez un compte PPPoE. Vous devez donc choisir **Oui**. Après avoir sélectionné l'option **Oui** et configuré votre routeur, il n'est pas nécessaire d'exécuter l'application PPP sur votre ordinateur pour établir la connexion à Internet.

a. Identifiant requis

Définissez les paramètres requis en fonction de votre connexion Internet. Les champs de cet écran sont décrits dans le *Tableau 23*.

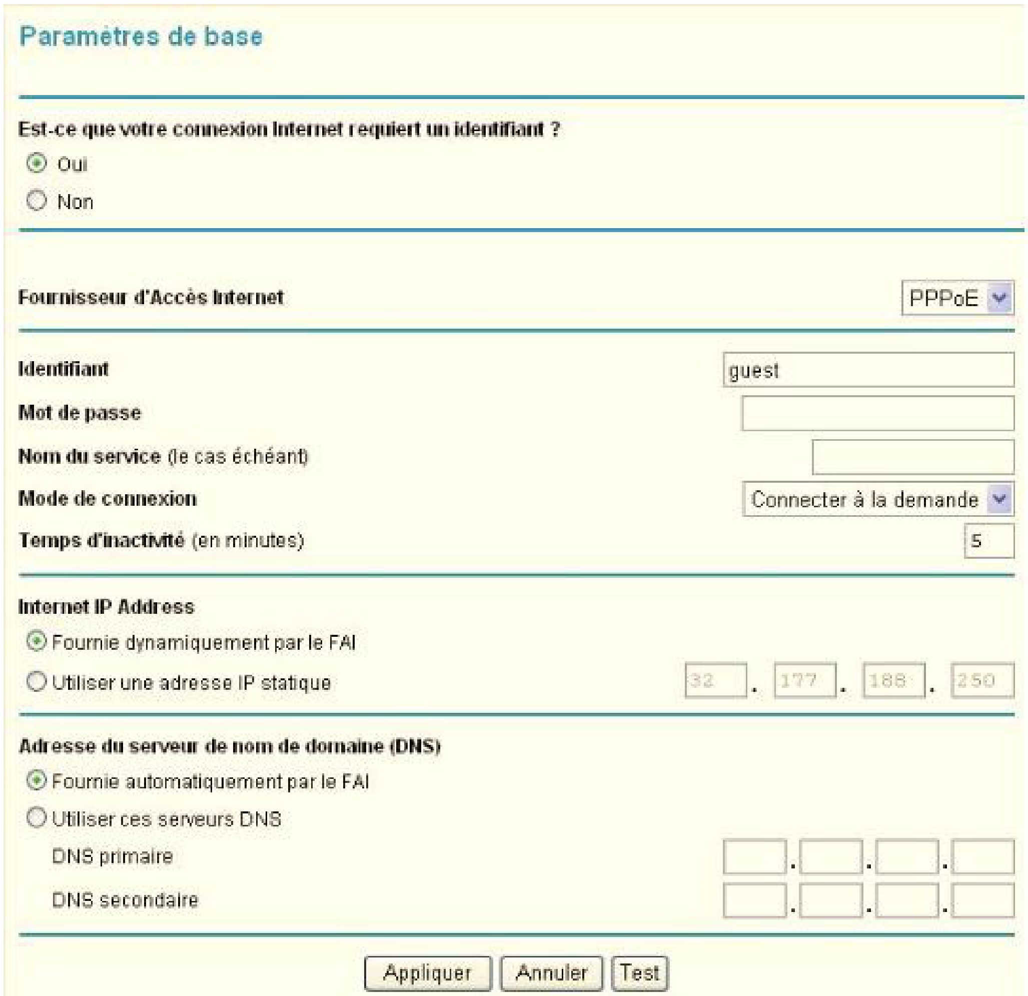


Tableau 4. Paramètres de connexion haut débit Ethernet lorsque l'identifiant est requis

Champs et cases à cocher	Description
Fournisseur d'accès Internet	Sélectionnez le service fourni par votre FAI. • PPPoE est le plus courant. • PPTP est utilisé en Autriche et dans d'autres pays d'Europe. • Telstra BigPond est utilisé en Australie seulement.
Identifiant	Il s'agit habituellement du nom utilisé dans votre adresse électronique. Par exemple, si l'adresse de votre compte de messagerie est DenisTremblay@ISP.com, alors entrez DenisTremblay dans ce champ. Certains FAI comme Mindspring, Earthlink et T-DSL exigent que vous utilisiez votre adresse électronique complète lorsque vous vous connectez. Dans ce cas, vous devez entrer l'adresse complète dans le champ **Identifiant**.

Tableau 4. Paramètres de connexion haut débit Ethernet lorsque l'identifiant est requis

Champs et cases à cocher	Description
Mot de passe	Tapez le mot de passe que vous utilisez pour vous connecter à votre FAI.
Nom du service (le cas échéant)	Si votre FAI vous a donné un nom de service, entrez-le ici. Sinon, vous pouvez laisser ce champ vide.
Mode de connexion	Sélectionnez le mode de connexion **Connecter à la demande**, **Always On** (Toujours connecté) ou **Manually Connect** (Connexion manuelle). • Avec le paramètre par défaut **Connecter à la demande** , une connexion PPPoE est automatiquement établie lorsqu'il y a un trafic sortant vers Internet, et elle est automatiquement rompue si la connexion est inactive pendant le délai indiqué dans le champ Temps d'inactivité. • Si le mode de connexion choisi est **Always On** (Toujours connecté), la connexion PPPoE est automatiquement établie lors du démarrage de l'ordinateur et elle n'est pas rompue après un certain délai d'inactivité. Si, pour une quelconque raison, la connexion est coupée, le routeur tentera continuellement de rétablir la connexion. • Si vous sélectionnez l'option **Manually Connect** (Connexion manuelle), vous devrez passer à l'écran Statut du routeur et cliquer sur le bouton **Connecter** pour établir la connexion Internet. La connexion manuelle n'est pas rompue après un certain délai d'inactivité et, si vous voulez vous déconnecter, vous devez cliquer sur le bouton **Déconnecter** dans l'écran Statut du routeur.
Temps d'inactivité (en minutes)	Une connexion Internet inactive sera interrompue après le délai indiqué. Si cette valeur est à zéro (0), le routeur maintiendra la connexion active en rétablissant immédiatement la connexion chaque fois qu'elle sera rompue.
Internet IP Address (Adresse IP Internet)	Si vous vous connectez à votre service ou si votre FAI ne vous a pas fourni d'adresse IP fixe, le routeur vous attribue automatiquement une adresse IP lorsque vous établissez la connexion. Sélectionnez **Fournie dynamiquement par le FAI**. Si vous avez une adresse IP fixe (statique, permanente), votre FAI devrait vous avoir attribué une adresse IP. Sélectionnez **Utiliser une adresse IP statique** et tapez l'adresse IP.
Adresse du serveur de nom de domaine (DNS)	Le serveur DNS est utilisé pour rechercher des adresses de sites à partir de leur nom. • Si votre FAI vous a donné une ou deux adresses DNS, sélectionnez **Utiliser ces serveurs DNS** et tapez les adresses DNS primaire et secondaire. • Sinon, sélectionnez **Fournie automatiquement par le FAI**. **Remarque** : si vous obtenez une erreur du type « Adresse introuvable » lorsque vous tentez d'accéder à un site Web, il se peut que vos serveurs DNS ne soient pas correctement configurés. Veuillez communiquer avec votre FAI pour obtenir les adresses de serveurs DNS.

b. Identifiant non requis

Définissez les paramètres requis en fonction de votre connexion Internet. Les champs de cet écran sont décrits dans le *Tableau 24*.

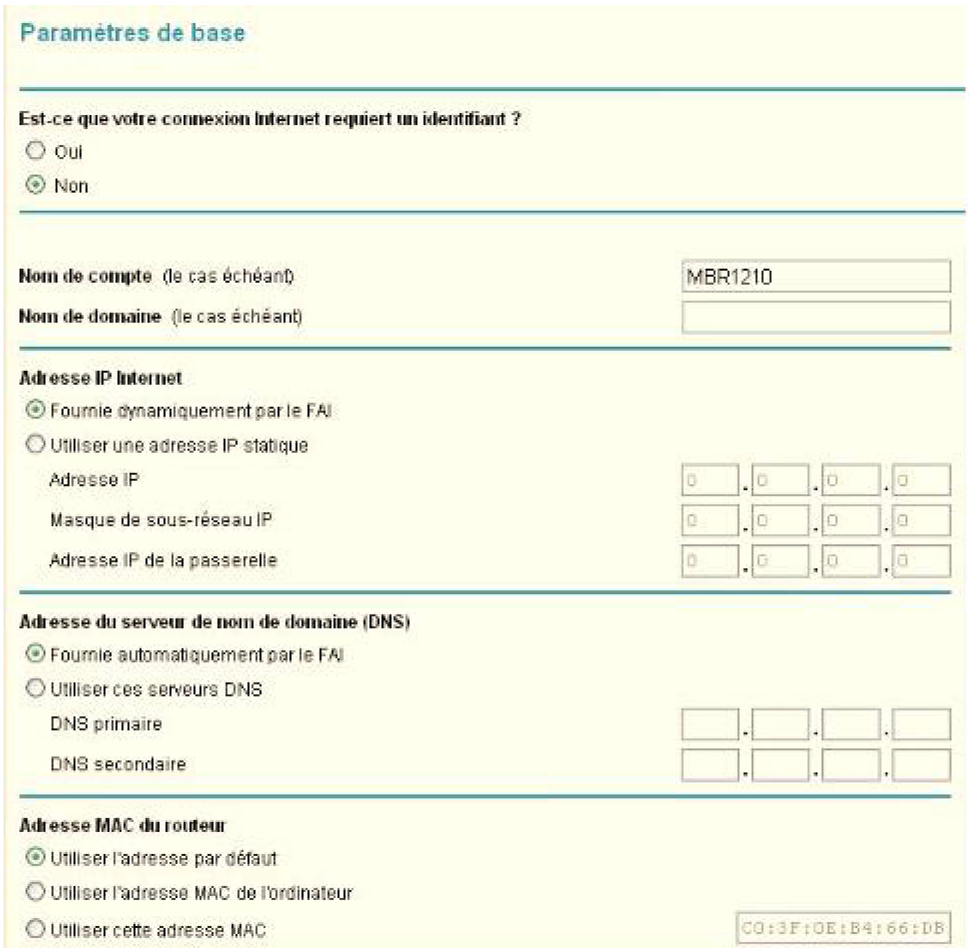


Tableau 5. Paramètres nede connexion haut débit Ethernet lorsque l'identifiant n'est pas requis

Champs et cases à cocher	Description
Nom du compte (le cas échéant)	Également appelé « nom d'hôte » ou « nom système ». Dans la plupart des cas, vous pouvez taper le nom de votre compte ou votre nom d'utilisateur dans ce champ. Par exemple, si l'adresse de votre compte de messagerie est DenisTremblay@ISP.com, alors entrez DenisTremblay dans ce champ. Si votre FAI vous a attribué un nom d'hôte spécifique, tapez-le dans ce champ (par exemple, CCA7324-A).
Nom de domaine (le cas échéant)	Dans la plupart des cas, vous pouvez laisser ce champ vide, sauf si cette valeur est requise par votre FAI. Vous pouvez taper le nom de domaine de votre FAI. Par exemple, si le serveur de messagerie de votre FAI est mail.xxx.yyy.zzz, vous devez taper xxx.yyy.zzz comme nom de domaine. Si votre FAI vous a attribué un nom de domaine, tapez-le dans ce champ. (Par exemple, la compagnie Earthlink Cable peut exiger un nom d'hôte du réseau domestique, et Comcast attribue parfois un nom de domaine.) Si vous utilisez un modem câble, ce nom correspond généralement à celui du groupe de travail.
Internet IP Address (Adresse IP Internet)	Si vous vous connectez à votre service ou si votre FAI ne vous a pas fourni d'adresse IP fixe, le routeur vous attribue automatiquement une adresse IP lorsque vous établissez la connexion. Sélectionnez **Fournie dynamiquement par le FAI**. Si vous avez une adresse IP fixe (ou statique), votre FAI devrait vous avoir donné les renseignements nécessaires. Sélectionnez **Utiliser une adresse IP statique** et tapez l'adresse IP, le masque de sous-réseau et l'adresse IP de la passerelle dans les champs appropriés. Par exemple : • **Adresse IP**. 24.218.156.183 • **Masque de sous-réseau** . 255.255.255.0 • **Adresse IP de la passerelle**. 24.218.156.1
Adresse du serveur de nom de domaine (DNS)	Le serveur DNS est utilisé pour rechercher des adresses de sites à partir de leur nom. • Si votre FAI vous a donné une ou deux adresses DNS, sélectionnez **Utiliser ces serveurs DNS** et tapez les adresses DNS primaire et secondaire. • Sinon, sélectionnez **Fournie automatiquement par le FAI**. **Remarque** : si vous obtenez une erreur du type « Adresse introuvable » lorsque vous tentez d'accéder à un site Web, il se peut que vos serveurs DNS ne soient pas correctement configurés. Veuillez communiquer avec votre FAI pour obtenir les adresses de serveurs DNS.

Tableau 5. Paramètres nede connexion haut débit Ethernet lorsque l'identifiant n'est pas requis (suite)

Champs et cases à cocher	Description
Adresse MAC du routeur	L'adresse locale de votre ordinateur est son adresse particulière sur votre réseau. Cette adresse est également appelée « adresse MAC » (*Media Access Control*). • En général, vous devez sélectionner **Utiliser l'adresse par défaut** . • Si votre FAI requiert une authentification MAC, sélectionnez **Utiliser l'adresse MAC de l'ordinateur** pour remplacer l'adresse MAC du routeur par celle de l'ordinateur, ou sélectionnez **Utiliser cette adresse MAC** pour taper manuellement l'adresse MAC d'un autre ordinateur. Le format de l'adresse MAC est XX:XX:XX:XX:XX:XX. Cette valeur peut être modifiée si vous sélectionnez l'option **Utiliser l'adresse MAC de l'ordinateur** après avoir déjà défini une valeur pour l'option **Utiliser cette adresse MAC**.

3. Voici les boutons disponibles :
   - **Appliquer**. Permet d'appliquer les modifications que vous avez apportées.
   - **Annuler**. Permet de rejeter les modifications en cours.
   - **Test**. Permet de tester la connexion au site Web NETGEAR. Si la connexion réussit, c'est que vos paramètres sont correctement définis. Vous pouvez alors cliquer sur **Déconnexion** pour fermer ces écrans.

2. Configuration du réseau sans fil

Pour une connexion sans fil, le SSID (aussi appelé nom de réseau sans fil) et les paramètres de sécurité sans fil doivent être identiques pour le router et les ordinateurs ou adaptateurs réseau sans fil. NETGEAR vous conseille fortement d'utiliser la sécurité sans fil.

Le routeur est préconfiguré au mode mixte WPA-PSK/WPA2-PSK et il utilise un SSID et une phrase d'authentification uniques. Cette information est imprimée sur l'étiquette située au bas du routeur. Utilisez cette information pour configurer vos ordinateurs et dispositifs WiFi.

Le présent chapitre décrit les points suivants :

- **Planification du réseau sans fil**
- **Configuration manuelle des paramètres sans fil**
- **Utilisation de la fonctionnalité « Appuyez : vous êtes connecté » (WPS) pour configurer votre réseau sans fil**

Remarque : Les ordinateurs peuvent se connecter par liaison sans fil depuis une distance de plusieurs centaines de pieds. Par conséquent, les personnes qui se trouvent à proximité de votre réseau pourront y accéder si vous n'utilisez pas la sécurité sans fil.

Planification du réseau sans fil

À des fins de conformité et de compatibilité entre les produits similaires se trouvant dans votre zone réseau, vous devez définir correctement le canal de fonctionnement et la région.

Pour configurer le réseau sans fil, vous pouvez soit spécifier manuellement les paramètres sans fil, soit utiliser la fonctionnalité Wi-Fi Protected Setup (WPS) pour définir automatiquement le SSID et mettre en place la sécurité WPA/WPA2.

- Pour configurer manuellement les paramètres sans fil, vous devez connaître les éléments suivants :
  - Le nom de réseau. Le SSID par défaut du router est NETGEAR-3G.
  - Le mode sans fil (802.11n, 802.11g ou 802.11b) pris en charge par chaque adaptateur réseau sans fil.
  - L’option de sécurité sans fil. Pour mettre en place la sécurité sans fil correctement, vérifiez chaque adaptateur sans fil afin de déterminer l’option de sécurité sans fil prise en charge.

  Consultez la section *Configuration manuelle des paramètres sans fil* à la page 129.
- La fonctionnalité « Appuyez : vous êtes connecté » (WPS) active la sécurité sans fil WPA/WPA2 à la fois sur le router et sur l'ordinateur ou le dispositif sans fil. L'ordinateur ou le dispositif sans fil doit être compatible avec la fonctionnalité WPS.

  Consultez la section *Utilisation de la fonctionnalité « Appuyez : vous êtes connecté » (WPS) pour configurer votre réseau sans fil* à la page 133.

Recommandations relatives à l'emplacement et à la portée des dispositifs sans fil

La portée de votre connexion sans fil peut varier considérablement en fonction de l’endroit où se trouve le router. Le temps d'attente du réseau, la performance du débit de données et la consommation d'énergie des adaptateurs réseau sans fil sur les ordinateurs portatifs peuvent aussi varier en fonction de votre configuration.

Pour des résultats optimaux, placez le router en respectant les recommandations suivantes :

- Près du centre de la zone de fonctionnement de vos ordinateurs.
- En hauteur (sur une étagère, par exemple), là où les ordinateurs connectés par liaison sans fil seront en ligne droite avec le routeur (même à travers les murs).
- Loin des sources d'interférences, comme les fours à micro-ondes et les téléphones sans fil à 2,4 GHz (consultez la section *Tableau de réduction du brouillage* à la page 201).
- Loin des grandes surfaces métalliques.
- Placez l'antenne à la verticale pour offrir la meilleure couverture à l'horizontale. Placez l'antenne à l'horizontale pour offrir la meilleure couverture à la verticale.
- Si vous utilisez plusieurs points d'accès, il est préférable que chacun utilise un canal de fréquences radio différent pour réduire les interférences. Le nombre de canaux recommandés entre chaque point d'accès est 5 (par exemple, utilisez les canaux 1 et 6 ou 6 et 11, etc.).

Le temps nécessaire à l'établissement d'une connexion sans fil peut varier selon vos paramètres de sécurité et l'emplacement du routeur. L'établissement d'une connexion WEP peut prendre un peu plus de temps. En outre, le chiffrement WEP peut épuiser plus rapidement la charge de la batterie sur un ordinateur portatif.

Options de sécurité sans fil

À l’intérieur d’un bâtiment, les ordinateurs peuvent se connecter à des réseaux sans fil 802.11n à une distance maximale de 300 pieds. Une telle distance pourrait permettre à des personnes qui se trouvent à l'extérieur, mais à proximité de votre réseau, d'y accéder.

Contrairement aux données de réseaux câblés, les transmissions de données sans fil peuvent s’étendre au-delà de vos murs et être reçues par toute personne à proximité disposant d’un adaptateur réseau compatible. Pour cette raison, activez les fonctions de sécurité de vos dispositifs sans fil. Le Mobile Broadband 11n Wireless Router offre des fonctions de sécurité hautement efficaces qui sont décrites en détail dans le présent chapitre. Déployez les fonctions de sécurité appropriées à vos besoins.

Chaque routeur est préconfiguré au mode mixte WPA-PSK/WPA2-PSK et utilise un SSID et une phrase d'authentification uniques.

Vous pouvez augmenter la sécurité de votre réseau sans fil de plusieurs façons :

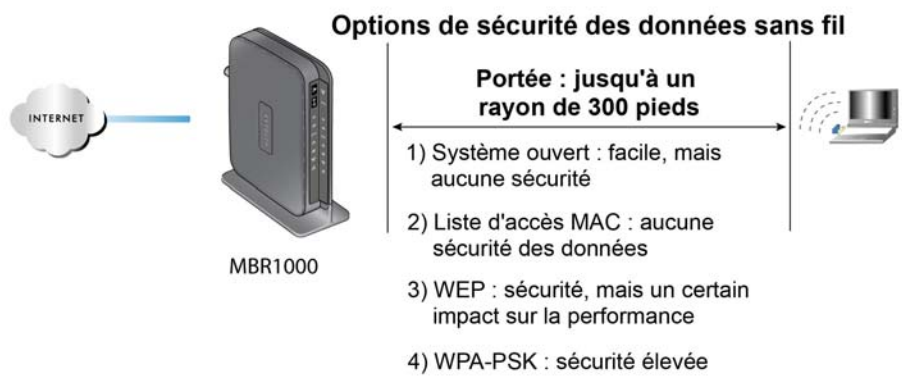


Figure 1. Sécurité sans fil

- **Limiter l'accès au moyen d'une adresse MAC**. Vous pouvez autoriser uniquement les ordinateurs de confiance à se connecter à votre réseau, de sorte que tout ordinateur inconnu ne pourra pas se connecter par liaison sans fil au router. Le fait de limiter l'accès au moyen d'une adresse MAC ajoute un obstacle aux tentatives d'intrusion, mais les données diffusées sur la liaison sans fil sont entièrement exposées.
- **Désactiver la fonction de diffusion du nom du réseau sans fil (SSID)**. Si vous désactivez la diffusion du SSID, seuls les dispositifs qui ont le SSID approprié peuvent se connecter. Cela annule la fonction de « détection » de réseaux sans fil de certains produits, comme Windows XP, mais les données sont tout de même exposées.
- **WEP.** Le chiffrement de données WEP (Wired Equivalent Privacy) procure une sécurité des données. L'authentification à clé partagée WEP et le chiffrement de données WEP bloquent tous les intrus, à l'exception des plus expérimentés. Ce mode de chiffrement de données a été supplanté par les modes WPA-PSK et WPA2-PSK.
- **WPA-PSK (TKIP), WPA2-PSK (AES)**. Le chiffrement Wi-Fi Protected Access (WPA) avec clé pré-partagée (pre-shared key, ou PSK) exécute les authentifications et génère les clés de chiffrement de données initiales. L'authentification vraiment plus robuste et la création dynamique d'une nouvelle clé pour chaque trame rendent pratiquement impossible toute intrusion.

Pour en savoir plus sur la technologie sans fil, cliquez sur le lien du document en ligne *Principes de base d'un réseau sans fil* à l’annexe A.

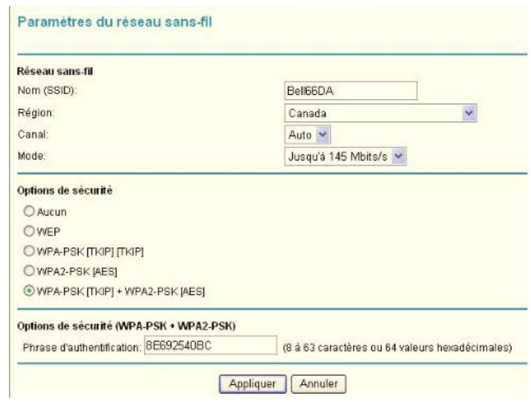
Configuration manuelle des paramètres sans fil

Remarque : Si vous utilisez un ordinateur connecté par liaison sans fil pour modifier le nom du réseau sans fil (SSID) ou les paramètres de sécurité sans fil, vous serez déconnecté lorsque vous cliquerez sur **Appliquer**. Pour éviter que cela ne se produise, connectez votre ordinateur au routeur à l'aide d'un câble Ethernet pour apporter vos modifications.

Pour afficher ou configurer manuellement les paramètres sans fil :

1. Connectez-vous au router en suivant les indications fournies dans la section *Connexion à votre routeur* à la page 113.
2. Sélectionnez Paramètres du réseau sans fil dans le menu principal.

   Les paramètres de cet écran sont décrits dans le *Tableau 25*.



3. Sélectionnez la région dans laquelle le router sera utilisé.
4. Pour la configuration initiale et la vérification, ne modifiez pas les autres paramètres.
5. Pour enregistrer vos modifications, cliquez sur **Appliquer**.
6. Configurez la connectivité sans fil de vos ordinateurs et vérifiez-la.

   Configurez vos ordinateurs sans fil avec les mêmes SSID et paramètres de sécurité sans fil que ceux de votre router. Vérifiez qu'ils disposent d'une liaison sans fil et qu'ils peuvent obtenir une adresse IP du router par l'intermédiaire du serveur DHCP. S'il y a des interférences, changez de canal.

Tableau 1.

Paramètres		Description
Réseau sans fil	Nom (SSID)	Le SSID est aussi appelé nom de réseau sans fil. Entrez un nom contenant un maximum de 32 caractères dans ce champ. Ce champ fait la distinction entre les majuscules et les minuscules. S'il y a plusieurs réseaux sans fil, le SSID procure un moyen de séparer le trafic. Pour joindre un réseau, un ordinateur ou un dispositif sans fil doit utiliser le SSID.
	Région	Emplacement où le router est utilisé.
	Canal	Canal sans fil utilisé par la passerelle. La valeur par défaut est **Auto**. Ne changez pas de canal, sauf s'il y a des interférences (que vous pouvez constater par des pertes de connexions ou des transferts de données ralentis). Le cas échéant, vous devez tester différents canaux pour trouver celui qui fonctionne le mieux.
	Mode	La valeur par défaut est Jusqu'à 145 Mbits/s.

Tableau 1

Paramètres		Description
Options de sécurité	Aucun	Utilisez ce paramètre pour établir la connectivité sans fil avant de mettre en place la sécurité du réseau sans fil. NETGEAR vous conseille fortement de sécuriser votre réseau sans fil.
	WEP	Utilisez des clés de chiffrement et le chiffrement des données pour sécuriser vos données. Vous pouvez sélectionner le chiffrement à 64 bits ou à 128 bits. Consultez la section *Configuration WEP* à la page 130.
	WPA-PSK (TKIP)	Permet uniquement aux ordinateurs configurés avec le protocole de sécurité WPA de se connecter au router. Consultez la section *Configuration WPA, WPA2 ou WPA + WPA2* à la page 132.
	WPA2-PSK (AES)	Permet uniquement aux ordinateurs configurés avec le protocole de sécurité WPA2 de se connecter au router. Consultez la section *Configuration WPA, WPA2 ou WPA + WPA2* à la page 132.
	WPA-PSK (TKIP), WPA2-PSK (AES)	Permet aux ordinateurs configurés avec le protocole de sécurité WPA-PSK ou WPA2-PSK de se connecter au router. Consultez la section *Configuration WPA, WPA2 ou WPA + WPA2* à la page 132.

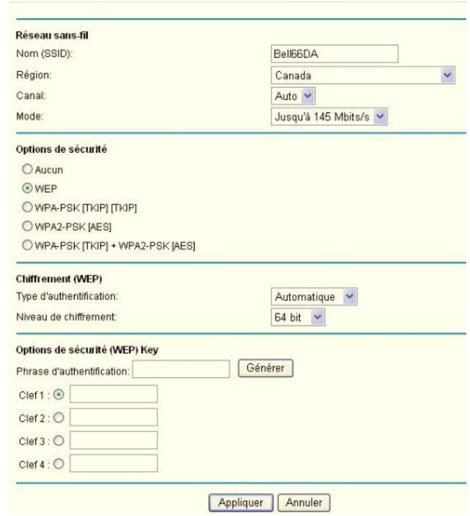
Configuration WEP

Remarque : Si vous utilisez un ordinateur connecté par liaison sans fil pour configurer les paramètres de sécurité sans fil, vous serez déconnecté lorsque vous cliquerez sur **Appliquer**. Reconfigurez votre ordinateur sans fil en fonction des nouveaux paramètres, ou accédez au router à partir d'un ordinateur câblé si vous devez apporter d'autres modifications.

Pour configurer le chiffrement de données WEP :

1. Connectez-vous au router en suivant les indications fournies dans la section *Connexion à votre routeur* à la page 113.
2. Dans le menu principal, sélectionnez Paramètres du réseau sans fil pour afficher cet écran.

3. Dans la section Options de sécurité, sélectionnez la case d'option **WEP** (Wired Equivalent Privacy) :



4. Définissez le paramètre **Type d'authentification** : **Automatique**, **Open System** (Système ouvert) ou **Shared Key** (Clé partagée). La valeur par défaut est **Open System** (Système ouvert).

   Remarque : *L'authentification est une opération distincte du chiffrement des données. Vous pouvez sélectionner une authentification qui nécessite une clé partagée, tout en ne chiffrant pas les transmissions de données. La sécurité est plus robuste si vous utilisez à la fois une clé partagée et le chiffrement WEP.*

5. Définissez le paramètre **Niveau de chiffrement** :
   - **64 bits**. Entrez 10 chiffres hexadécimaux (toute combinaison de 0 à 9, a à f ou A à F).
   - **128 bits**. Entrez 26 chiffres hexadécimaux (toute combinaison de 0 à 9, a à f ou A à F).

6. Entrez les clés de chiffrement. Vous pouvez programmer manuellement ou automatiquement les quatre clés de chiffrement de données. Ces valeurs doivent être identiques sur tous les ordinateurs et points d'accès de votre réseau :
   - **Phrase d'authentification**. Pour utiliser une phrase d'authentification afin de générer les clés, entrez cette phrase et cliquez sur **Générer**. Les clés sont créées automatiquement. Les stations sans fil doivent utiliser la phrase d'authentification ou les clés pour accéder au router.

   Remarque : *Les adaptateurs réseau sans fil ne prennent pas tous en charge la génération de clés au moyen d'une phrase d'authentification.*

   - **Clef 1–Clef 4**. Le système ne fait *pas* la distinction entre les majuscules et les minuscules pour ces valeurs. Vous pouvez entrer manuellement les quatre clés de chiffrement de données. Ces valeurs doivent être identiques sur tous les ordinateurs et points d'accès de votre réseau. Entrez 10 chiffres hexadécimaux (toute combinaison de 0 à 9, a à f ou A à F).

7. Sélectionnez la clé qui sera celle par défaut.

   Les transmissions de données sont toujours chiffrées au moyen de la clé par défaut. Les autres clés peuvent être utilisées seulement pour déchiffrer les données reçues. Les quatre champs de clé sont désactivés si l'authentification sélectionnée est WPA-PSK ou WPA.

8. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

Configuration WPA, WPA2 ou WPA + WPA2

Les protocoles de sécurité WPA et WPA2 procurent une sécurité des données très robuste. Le protocole WPA utilisant TKIP est une mise en œuvre logicielle qui peut être utilisée sur les systèmes Windows Service Pack 2 ou version ultérieure, tandis que le protocole WPA2 utilisant AES est une mise en œuvre matérielle. Consultez la documentation de votre dispositif avant d'effectuer la mise en œuvre. Consultez la documentation de votre adaptateur réseau sans fil pour obtenir les instructions de configuration des paramètres WPA.

Remarque : Si vous utilisez un ordinateur connecté par liaison sans fil pour configurer les paramètres de sécurité sans fil, vous serez déconnecté lorsque vous cliquerez sur **Appliquer**. Le cas échéant, reconfigurez votre ordinateur sans fil en fonction des nouveaux paramètres, ou accédez au router à partir d'un ordinateur câblé si vous devez apporter d'autres modifications.

Pour configurer les protocoles WPA ou WPA2 sur le router :

1. Connectez-vous au router en suivant les indications fournies dans la section *Connexion à votre routeur* à la page 113.
2. Sélectionnez Paramètres du réseau sans fil dans le menu principal.
3. Dans l'écran Paramètres du réseau sans fil, sélectionnez la case d'option WPA ou WPA2 de votre choix.
4. Pour WPA-PSK et WPA2-PSK, entrez la phrase d'authentification.
5. Pour sauvegarder vos paramètres, cliquez sur **Appliquer**.

Utilisation de la fonctionnalité « Appuyez : vous êtes connecté » (WPS) pour configurer votre réseau sans fil

Pour utiliser la fonctionnalité « Appuyez : vous êtes connecté », vos ordinateurs ou dispositifs sans fil doivent prendre en charge la fonctionnalité Wi-Fi Protected Setup (WPS). Les appareils compatibles portent généralement le symbole WPS .
La fonctionnalité WPS peut configurer le nom du réseau sans fil (SSID) et la sécurité sans fil WPA/WPA2 à la fois pour le router et pour l'ordinateur ou le dispositif sans fil.

Points à considérer sur la WPS :

- La fonctionnalité « Appuyez : vous êtes connecté » de NETGEAR repose sur la norme WPS. Tous les autres produits compatibles Wi-Fi et WPS doivent prendre en charge les produits NETGEAR qui offrent la fonctionnalité « Appuyez : vous êtes connecté ».
- Si vous envisagez de créer un réseau combiné de périphériques compatibles et non compatibles avec WPS, NETGEAR vous recommande de configurer d'abord votre réseau sans fil et vos paramètres de sécurité manuellement, puis d'utiliser WPS uniquement pour ajouter les dispositifs compatibles WPS.

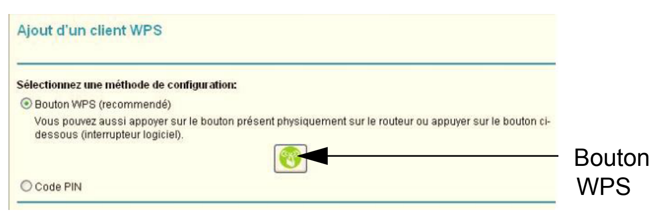
Bouton WPS

Tout ordinateur ou adaptateur réseau sans fil qui est connecté au router par liaison sans fil est considéré comme un client. Le client doit disposer d'un bouton WPS ainsi que d'un utilitaire de configuration WPS, comme l'assistant de configuration NETGEAR ou Atheros Jumpstart.

Pour utiliser le bouton WPS du router pour ajouter un client WPS :

1. Connectez-vous au router en suivant les indications fournies dans la section *Connexion à votre routeur* à la page 113.
2. Dans le menu principal du router, sélectionnez Ajout d'un client WPS, puis cliquez sur **Suivant**.

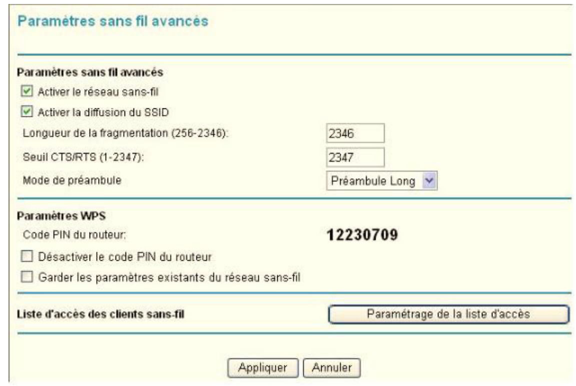
   La case d'option **Bouton WPS (recommandé)** est sélectionnée par défaut.



3. Cliquez sur le bouton à l'écran ou appuyez sur le bouton WPS situé sur le devant du router.

   Le router essaie de communiquer avec le client (c'est-à-dire avec l'ordinateur qui désire joindre le réseau) pendant deux minutes.
4. Sur l'ordinateur sans fil client, exécutez un utilitaire de configuration WPS. Suivez les instructions de l'utilitaire pour cliquer sur le bouton WPS.
5. Revenez à l'écran du router pour vérifier la présence d'un message.

L'écran WPS du router affiche un message confirmant que le client a été ajouté au réseau sans fil. Le router génère un SSID et met en place la sécurité WPA/WPA2. Le router conserve ces paramètres sans fil, à moins que vous ne les modifiiez ou que vous ne décochiez la case **Garder les paramètres existants du réseau sans fil**, dans la section Paramètres WPS de l'écran Paramètres sans fil avancés.



6. Notez le nouveau nom de réseau (SSID) et le mot de passe WPA/WPA2 du réseau sans fil. Ces paramètres sont indiqués dans l'écran Paramètres du réseau sans fil. Consultez la section *Configuration manuelle des paramètres sans fil* à la page 129.

Pour accéder à Internet depuis un ordinateur connecté à votre router, lancez un navigateur comme Microsoft Internet Explorer ou Firefox. Le voyant Internet de votre router devrait clignoter pour indiquer qu'il communique avec le fournisseur d'accès et

Remarque : Si aucun dispositif client compatible WPS n'est trouvé pendant le délai de deux minutes, le SSID ne change pas et aucune fonction de sécurité n'est configurée.

Entrée d'un code PIN WPS

Tout ordinateur ou dispositif sans fil qui est connecté au router par liaison sans fil est considéré comme un client. Le client doit prendre en charge les codes PIN WPS et disposer d'un utilitaire de configuration WPS, comme l’assistant de configuration NETGEAR ou Atheros Jumpstart.

La première fois que vous ajoutez un client WPS, assurez-vous que la case **Garder les paramètres existants du réseau sans fil** n'est pas cochée, dans la section Paramètres WPS. Il s'agit du paramètre par défaut pour le router, qui peut ainsi générer le SSID et les paramètres de sécurité WPA/WPA2 au moyen de la fonctionnalité WPS. Une fois que la fonctionnalité WPS a été exécutée, le router coche automatiquement cette case afin que le SSID et les paramètres de sécurité sans fil soient conservés si vous ajoutez d'autres dispositifs WPS par la suite.

Pour utiliser un code PIN lors de l'ajout d'un client WPS :

1. Connectez-vous au router en suivant les indications fournies dans la section *Connexion à votre routeur* à la page 113.
2. Dans le menu principal du router, sélectionnez Ajout d'un client WPS (les ordinateurs qui se connectent par liaison sans fil au router sont des clients), puis cliquez sur **Suivant**. L’écran Ajout d'un client WPS apparaît.



3. Sélectionnez la case d'option **Code PIN**.
4. Rendez-vous à l'ordinateur sans fil client. Exécutez un utilitaire de configuration WPS. Suivez les instructions de l'utilitaire pour générer un code PIN. Notez le code PIN du client.
5. Dans l'écran Ajout d'un client WPS du router, entrez le code PIN du client puis cliquez sur **Suivant**.
   - Le router tente de communiquer avec le client pendant quatre minutes. Si aucun client WPS ne se connecte au cours de cette période, les paramètres sans fil du router ne changent pas.
   - L'écran WPS du router affiche un message confirmant que le client a été ajouté au réseau sans fil. Le router génère un SSID et met en place la sécurité WPA/WPA2.
6. Notez le nouveau nom de réseau (SSID) et le mot de passe WPA/WPA2 du réseau sans fil. Ces paramètres sont indiqués dans l'écran Paramètres du réseau sans fil. Consultez la section *Configuration manuelle des paramètres sans fil* à la page 129.

Pour accéder à Internet à partir d'un ordinateur connecté à votre router, lancez un navigateur comme Microsoft Internet Explorer ou Mozilla Firefox. Le voyant Internet du router devrait clignoter.

Ajout d'ordinateurs sans fil qui ne prennent pas en charge la fonctionnalité WPS

Si vous avez configuré votre réseau au moyen de la fonctionnalité WPS et que vous souhaitez ajouter un ordinateur qui ne prend pas en charge WPS, vous devez configurer manuellement cet ordinateur. Pour en savoir plus sur l'affichage des paramètres sans fil du routeur, consultez la section *Configuration manuelle des paramètres sans fil* à la page 129.

Le SSID et les clés WPA/WPA2 étant créés aléatoirement par le protocole WPA. Il pourrait donc s'avérer difficile de les taper ou de les mémoriser (c'est l'une des raisons pour lesquelles le réseau est si sécuritaire). Vous pouvez modifier les paramètres sans fil de façon à ce qu'ils soient plus faciles à mémoriser. Le cas échéant, vous devrez reconfigurer les ordinateurs compatibles WPS.

Remarque : La modification des paramètres sans fil déconnectera tous les ordinateurs sans fil du réseau. Vous devrez alors les reconfigurer avec les nouveaux paramètres sans fil.

Pour modifier les paramètres sans fil du réseau :

1. Utilisez un câble Ethernet pour connecter un ordinateur au routeur. De cette façon, vous ne serez pas déconnecté lors de la modification des paramètres sans fil.
2. Connectez-vous au routeur et sélectionnez Paramètres du réseau sans fil (consultez la section *Configuration manuelle des paramètres sans fil* à la page 129).
3. Apportez les modifications suivantes :
   - Remplacez le nom du réseau sans fil (SSID) par un nom plus significatif.
   - Dans la section Options de sécurité (WPA/PSK + WPA2/PSK), sélectionnez une phrase d'authentification.
   - Assurez-vous que la case **Garder les paramètres existants du réseau sans fil** est cochée dans la section Paramètres WPS. Ainsi, vos nouveaux paramètres ne seront pas effacés si vous utilisez la fonctionnalité WPS.
4. Cliquez sur **Appliquer** pour instaurer vos modifications. Notez vos paramètres.

   Tous les clients sans fil existants sont dissociés et déconnectés du router.
5. Pour les dispositifs non compatibles WPS que vous désirez connecter, ouvrez l'utilitaire de réseau et suivez ses instructions pour entrer les paramètres de sécurité que vous avez sélectionnés à l'étape 3 (le SSID, le mode de sécurité WPA/PSK + WPA2/PSK et la phrase d'authentification).
6. Pour les dispositifs WPS que vous souhaitez connecter, suivez la procédure *Bouton WPS* à la page 133 ou *Entrée d'un code PIN WPS* à la page 135.

   Les paramètres que vous avez configurés à l'étape 3 sont diffusés sur les dispositifs WPS pour qu'ils puissent se connecter au router.

Code PIN de carte SIM

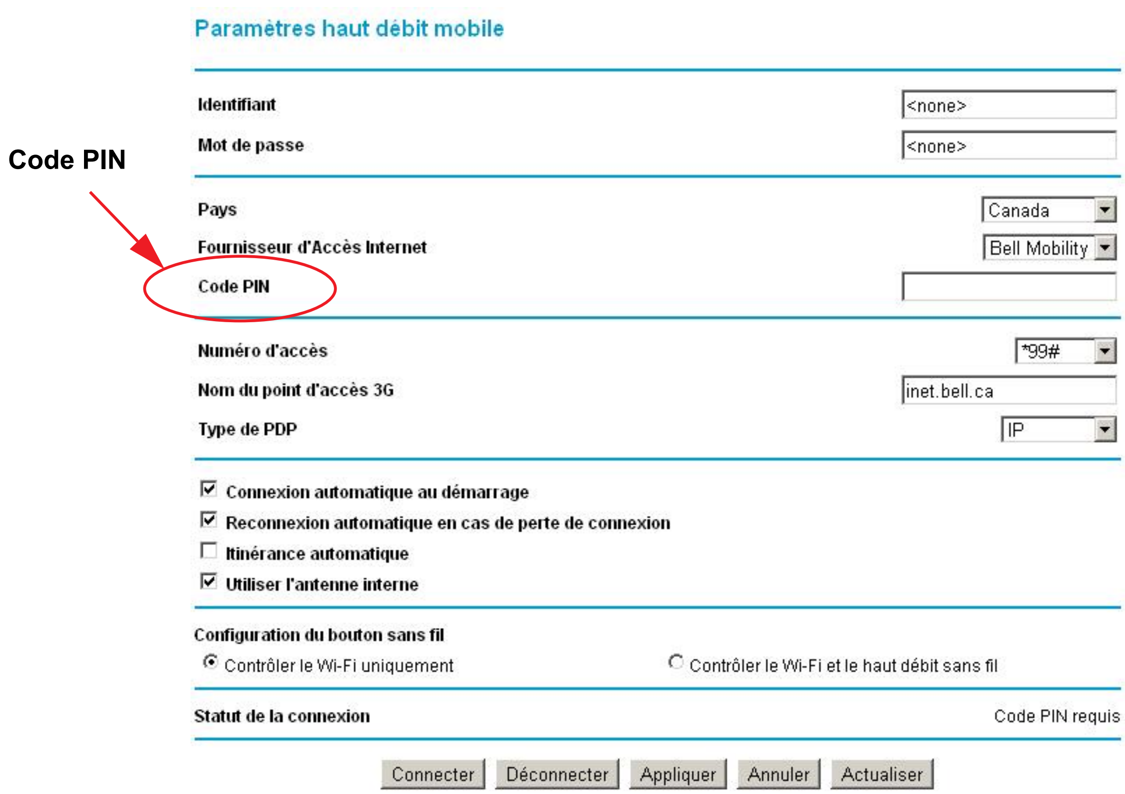
Certaines cartes SIM disposent d'un code PIN. Sans ce code, vous ne pouvez pas accéder à Internet. Le message ci-dessous s'affiche si un code PIN est requis, mais n'a pas encore été entré.



Pour entrer le code PIN :

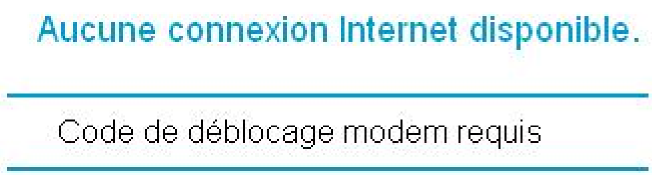
1. Connectez-vous au routeur et sélectionnez **Paramètres haut débit mobile** dans la section Configuration.
2. Entrez le code PIN.

   Si vous ignorez le code PIN, informez-vous auprès du fabricant du routeur.



Code de déverrouillage du modem d'une carte SIM

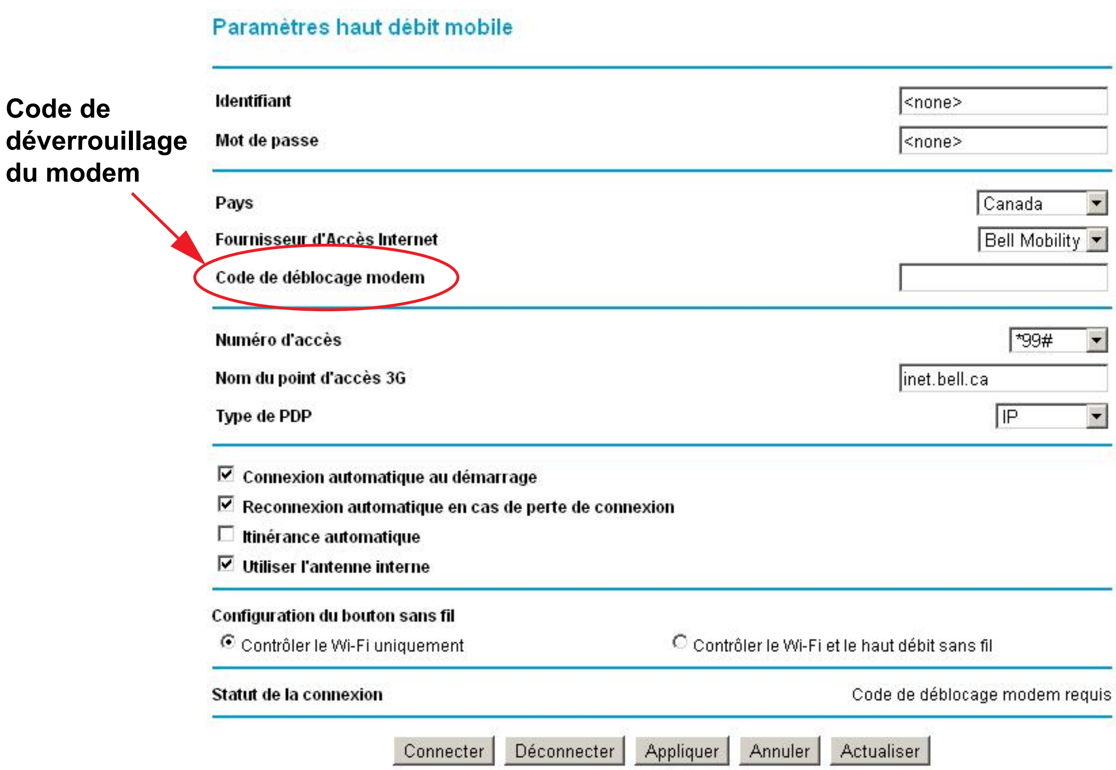
Si vous disposez d'une carte SIM n'ayant pas été fournie par le détaillant qui vous a vendu le routeur, vous pourriez obtenir un message d'erreur indiquant que le modem est verrouillé. Vous devez entrer un code de déverrouillage pour continuer.



Pour entrer le code de déverrouillage du modem :

1. Connectez-vous au routeur et sélectionnez **Paramètres haut débit mobile** dans la section Configuration.
2. Entrez le code de déverrouillage du modem.

   Vous pouvez obtenir ce code de déverrouillage en vous adressant au fabricant du routeur.



3. Filtrage de contenu

3

Ce chapitre explique comment utiliser les fonctions de base de pare-feu du router pour protéger votre réseau.

- **Affichage, sélection et enregistrement des données de journaux**
- **Blocage de sites et mots clefs**
- **Blocage de services**
- **Planning**
- **Activation de la notification par courriel des événements de sécurité**

Remarque : Pour en savoir plus sur les fonctions avancées de filtrage de contenu Ouverture de port et Déclenchement de port, consultez la section *Ouverture de port et déclenchement de port* à la page 166.

Affichage, sélection et enregistrement des données de journaux

Le router enregistre les événements relatifs à la sécurité, comme les demandes de service refusées, les tentatives d'intrusion et les connexions d'administrateur. Si vous avez activé le filtrage de contenu à l'écran Blocage de sites, l'écran Journaux peut s'afficher lorsqu'une personne de votre réseau tente d'accéder à un site bloqué.

Dans le menu principal, sous Filtrage de contenu, sélectionnez Journaux pour accéder à l'écran suivant :

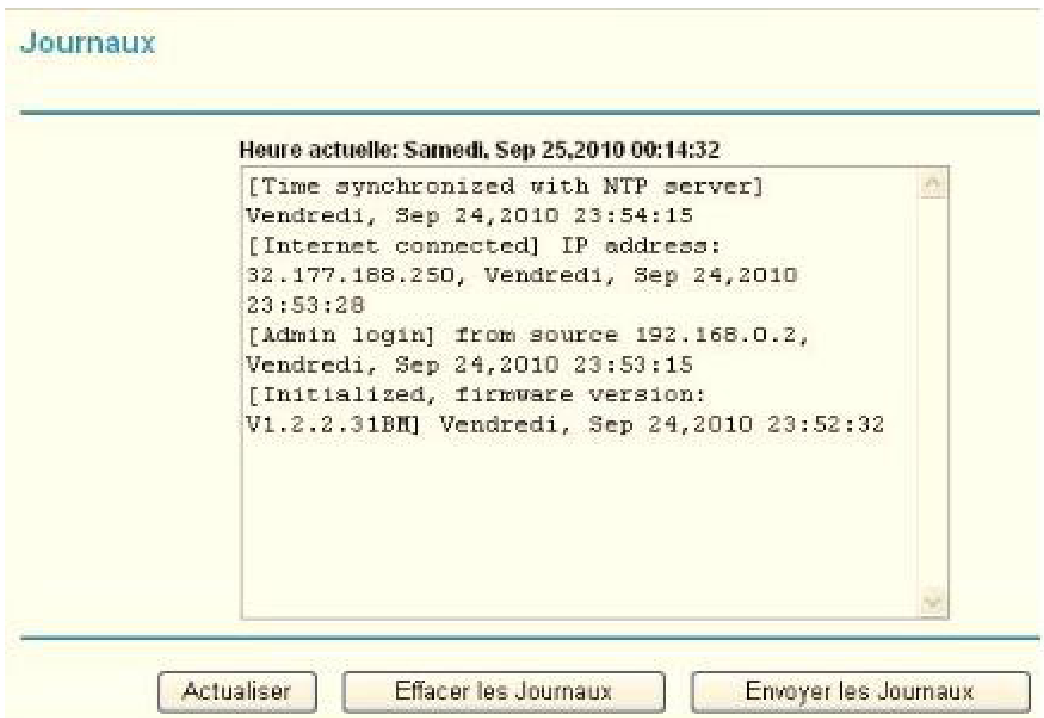


Figure 1.

Remarque : Vous pouvez activer la notification par courriel pour recevoir ces journaux dans un message électronique. Consultez la section *Activation de la notification par courriel des événements de sécurité* à la page 147.

Les entrées de journal et les boutons de commande sont décrits dans le *Tableau 26*.

Tableau 1.

Champ ou bouton	Description
Heure actuelle	Heure et date d'enregistrement de l'entrée de journal.
Description ou action	Type d'événement et action entreprise, s'il y a lieu.
Source IP (IP source)	Adresse IP du périphérique qui a déclenché l'entrée de journal.
Source port and interface (Port et interface source)	Numéro du port de maintenance du périphérique qui a déclenché l'entrée de journal et indication du type de réseau (local ou étendu).
Destination	Nom ou adresse IP du périphérique ou du site Web de destination.
Destination port and interface (Port et interface de destination)	Numéro du port de maintenance du périphérique de destination et indication du type de réseau (local ou étendu).
Bouton Actualiser	Permet d'actualiser les données de l'écran Journaux.
Bouton Effacer les journaux	Permet d'effacer les entrées de journal.
Bouton Envoyer les journaux	Permet d'envoyer immédiatement le fichier journal.
Bouton Appliquer	Permet d'appliquer les paramètres actuels.
Bouton Annuler	Permet d'effacer les paramètres actuels.

Sélection des données à consigner dans les journaux

En plus des renseignements standard indiqués précédemment, vous pouvez choisir d'enregistrer d'autres données dans les journaux. Voici les autres options offertes :

- Attempted access to blocked site (Tentative d'accès à un site bloqué)
- Connections to the router menu (Connexions au menu du routeur)
- Router operation (start up, get time, and so on) (Fonctionnement du routeur – démarrage, obtention de l'heure, etc.)
- Attaques par déni de service et balayages de ports

Sauvegarde des fichiers journaux sur un serveur

Vous pouvez sauvegarder les journaux sur un ordinateur au moyen d'un programme de journal système. Pour activer cette fonction, sélectionnez la case d'option **Broadcast on LAN** (Diffuser sur le réseau local), ou entrez l'adresse IP du serveur sur lequel le fichier de journal système sera sauvegardé.

Exemples de messages de journal

Voici des exemples de messages de journal. Dans tous les cas, la date et l'heure sont indiquées comme suit dans l'entrée de journal : jour, année-mois-date heure:minute:seconde.

Activation et administration

```
Tue, 2002-05-21 18:48:39 - NETGEAR activated
```

Cette entrée indique une mise sous tension ou un redémarrage, ainsi que la date et l'heure à laquelle il s'est produit.

`Tue, 2002-05-21 18:55:00 - Administrator login successful - IP:192.168.0.2`

`Thu, 2002-05-21 18:56:58 - Administrator logout - IP:192.168.0.2`

Cette entrée indique la connexion et la déconnexion d'un administrateur pour l'adresse IP 192.168.0.2.

```
Tue, 2002-05-21 19:00:06 - Login screen timed out - IP:192.168.0.2
```

Cette entrée indique la fermeture d'une session d'administrateur en raison du délai de déconnexion.

```
Wed, 2002-05-22 22:00:19 - Log emailed
```

Cette entrée indique la date et l'heure de l'envoi du journal par courriel.

Paquets abandonnés

```
Wed, 2002-05-22 07:15:15 - TCP packet dropped - Source:64.12.47.28,4787,WAN -
Destination:134.177.0.11,21,LAN - [Inbound Default rule match]
```

```
Sun, 2002-05-22 12:50:33 - UDP packet dropped - Source:64.12.47.28,10714,WAN -
Destination:134.177.0.11,6970,LAN - [Inbound Default rule match]
```

```
Sun, 2002-05-22 21:02:53 - ICMP packet dropped - Source:64.12.47.28,0,WAN -
Destination:134.177.0.11,0,LAN - [Inbound Default rule match]
```

Ces entrées indiquent que les paquets FTP entrants (sur le port 21), les paquets User Datagram Protocol (UDP) (sur le port 6970) et les paquets Internet Control Message Protocol (ICMP) (sur le port 0) ont été abandonnés en raison d'une règle par défaut relative aux données entrantes, qui stipule que tous les paquets entrants doivent être refusés.

Blocage de sites et mots clefs

Le router offre plusieurs options de blocage de contenu Internet et de services de communications. Avec sa fonction de filtrage de contenu, le router empêche que du contenu inapproprié soit chargé sur votre ordinateur. Vous pouvez contrôler l'accès au contenu Internet en bloquant des sites selon des mots clefs se trouvant dans des adresses Web. Les options de filtrage de contenu comprennent :

- Blocage par mot clef du trafic HTTP.
- Blocage de service sortant. Limite l'accès de votre réseau local aux sites ou services Internet que vous précisez comme étant interdits.
- Protection des attaques de déni de service. Détecte et contrecarre les attaques par déni de service de type « Ping of death », « SYN flood », « LAND attack » et usurpation d'adresse IP.
- Blocage du trafic indésirable provenant d'Internet sur votre réseau local.

Le router vous permet de limiter l'accès au contenu Internet en fonction d'adresses Web et de mots clefs contenus dans les adresses.

1. Connectez-vous au router en suivant les indications fournies dans la section *Connexion à votre routeur* à la page 113.
2. Dans le menu principal, sélectionnez Blocage de sites pour afficher cet écran.



3. Pour activer le blocage par mot clef, sélectionnez l'une des options suivantes :
   - **Selon planning**. Active le blocage par mot clef en fonction des paramètres définis à l'écran Planning.
   - **Toujours**. Active le blocage par mot clef en tout temps, quels que soient les paramètres définis à l'écran Planning.
4. Entrez un mot clef ou un nom de domaine dans le champ de **mot clef** et cliquez sur **Ajout** puis sur **Appliquer**.

Le tableau suivant présente quelques exemples d'utilisation de mots clefs.

Tableau 2.

Mot clef	Résultat
XXX	Bloque l'URL http://www.mauvaiscontenu.com/xxx.html.
.com	Seuls les sites Web ayant un autre suffixe de nom de domaine que .com peuvent être consultés (.edu, .gov, etc.).
. (un point)	Bloque tout accès à la navigation Internet.

La liste de mots clefs peut contenir jusqu'à 32 entrées.

Remarque : Si vous bloquez des sites, vous pouvez configurer le router de façon à ce qu'il consigne dans un journal les tentatives d'accès à ces sites. Consultez la section *Affichage, sélection et enregistrement des données de journaux* à la page 140.

5. Pour supprimer un mot clef ou un nom de domaine, sélectionnez-le dans la liste et cliquez sur **Effacer**, puis sur **Appliquer**.
6. Pour spécifier un utilisateur de confiance, entrez l'adresse IP de son ordinateur dans le champ **Adresse IP approuvée**, puis cliquez sur **Appliquer**.

   Un utilisateur de confiance représente un ordinateur désigné qui sera exempt de tout blocage. Comme l'utilisateur de confiance est identifié par une adresse IP, son ordinateur devrait être configuré au moyen d'une adresse IP statique.
7. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

Blocage de services

1. Connectez-vous au router en suivant les indications fournies dans la section *Connexion à votre routeur* à la page 113.
2. Dans le menu principal, sous Filtrage de contenu, sélectionnez Bloquer des services pour accéder à cet écran.



Figure 2.

3. Sélectionnez l'une des options suivantes :
   - **Selon planning**. Active le blocage par mot clef en fonction des paramètres définis à l'écran Planning.
   - **Toujours**. Active le blocage par mot clef en tout temps, quels que soient les paramètres définis à l'écran Planning.
4. Cliquez sur **Ajouter**. L'écran suivant apparaît :

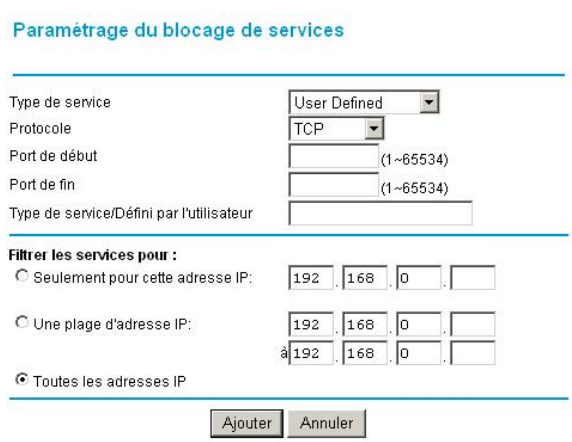


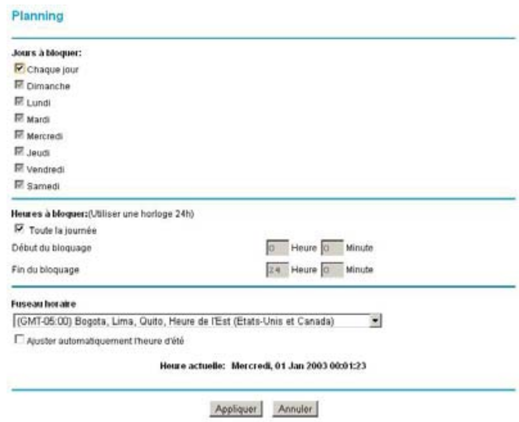
Figure 3.

5. Sélectionnez un service dans la liste déroulante **Service Type** (Type de service) ou définissez un service personnalisé dans le champ **Service/Type User Defined** (Service/Type défini par l'utilisateur).
6. Cliquez sur **Ajout** pour créer le service. Celui-ci sera affiché dans la section Tableau des services, à l'écran Bloquer des services.
7. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

Planning

Le router utilise le protocole de synchronisation réseau NTP pour obtenir la date et l'heure courantes d'un des nombreux serveurs temporels réseau sur Internet.

Configuration de votre fuseau horaire



Pour que l'heure indiquée dans vos entrées de journal corresponde à votre heure locale, vous devez indiquer votre fuseau horaire :

1. Connectez-vous au router en suivant les indications fournies dans la section *Connexion à votre routeur* à la page 113.
2. Dans le menu principal, sous Filtrage de contenu, sélectionnez Planning.
3. Sélectionnez votre fuseau horaire. Ce paramètre sera appliqué aux horaires de blocage dans votre fuseau horaire local et pour l'horodatage des entrées de journal.

   Si vous observez l'heure avancée dans votre fuseau horaire, cochez la case **Automatically adjust for daylight savings time** (Ajustement automatique à l'heure avancée).
4. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

Programmation des services de pare-feu

Si vous avez activé le blocage de services dans l'écran Bloquer des services, ou activé l'ouverture de port dans l'écran Ports, vous pouvez configurer un programme qui détermine quand le blocage doit être appliqué ou quand l'accès ne sera pas limité.

1. Connectez-vous au router en suivant les indications fournies dans la section *Connexion à votre routeur* à la page 113.
2. Dans le menu principal, sélectionnez Planning. L'écran Planning apparaît.
3. Pour bloquer les services Internet en fonction d'un horaire particulier, choisissez **Every Day** (Tous les jours), ou bien sélectionnez un ou plusieurs jours. Si vous souhaitez limiter totalement l'accès durant les jours sélectionnés, choisissez **All Day** (Toute la journée). Sinon, pour limiter l'accès à certaines heures durant les journées sélectionnées, entrez une valeur dans les champs **Start Blocking** (Début du blocage) et **End Blocking** (Fin du blocage).
4. Entrez ces valeurs dans le format 24 heures. Par exemple, 10:30 a.m. correspond à 10 h 30, et 10:30 p.m. correspond à 22 h 30. Si vous indiquez une heure de début qui est ultérieure à l'heure de fin, l'horaire sera en vigueur jusqu'à minuit le lendemain.
5. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Activation de la notification par courriel des événements de sécurité

Pour configurer le routeur de façon à ce que vous puissiez recevoir des journaux et des alertes par courriel, sélectionnez E-mail dans le menu principal pour afficher l'écran suivant :



Pour recevoir des alertes et des journaux par courriel :

1. Cochez la case **Activer la notification par e-mail**.
2. Remplissez les champs pour l'envoi d'alertes et de journaux par courriel.
   - **Serveur mail sortant**. Entrez le nom ou l'adresse IP du serveur de messagerie SMTP sortant de votre FAI (ex. courriel.monFAI.com).
   - **Envoyer à cette adresse e-mail.** Entrez l'adresse électronique à laquelle les alertes et les journaux seront envoyés. Entrez l'adresse complète, comme ChrisXY@monFAI.com.
   - **Mon serveur mail requiert une authentification**. Cochez cette case si vous devez vous connecter à votre serveur SMTP pour envoyer un courriel. Si vous sélectionnez cette fonction, vous devez entrer l'identifiant et le mot de passe de l'utilisateur pour le serveur de messagerie.

   Conseil : Si vous avez oublié ces données, vérifiez les paramètres dans votre programme de messagerie.

3. Indiquez à quel moment les alertes et les journaux seront envoyés :
   - **Envoyer l'alerte immédiatement**. Cochez cette case si vous désirez être avisé sur-le-champ de tout événement de sécurité important, comme une attaque connue, un balayage de ports ou une tentative d'accès à un site bloqué.
   - **Envoyer les journaux en suivant cette planification**. Précisez l'intervalle d'envoi des journaux : **Hourly** (Chaque heure), **Daily** (Quotidien), **Weekly** (Hebdomadaire) ou **When Full** (Lorsque plein).
   - **Jour (d'envoi du journal)**. Indique à quel jour de la semaine le journal est envoyé. Cette option est pertinente si les journaux sont envoyés une fois par semaine.
   - **Heure (d'envoi du journal)**. Indique à quelle heure le journal est envoyé. Cette option est pertinente si les journaux sont envoyés chaque jour ou chaque semaine.

   Si vous sélectionnez l'option **Weekly** (Hebdomadaire), **Daily** (Quotidien) ou **Hourly** (Chaque heure) et que le journal est plein avant la période indiquée, le journal est envoyé automatiquement par courriel à l'adresse entrée. Après l'envoi du journal, celui-ci est effacé de la mémoire du router. Si le router ne parvient pas à envoyer par le fichier journal, la mémoire tampon du journal pourrait être pleine. Dans ce cas, le router remplace le journal et efface son contenu.

4. Cliquez sur **Appliquer** pour instaurer vos modifications.

4. Gestion de votre réseau

Ce chapitre explique comment effectuer les tâches de gestion de réseau au moyen de votre Mobile Broadband 11n Wireless Router.

- **Statut du routeur**
- **Sauvegarde, restauration ou effacement de vos paramètres**
- **Protection de l'accès à votre Router**
- **Exécution d'utilitaires de diagnostic et redémarrage du routeur**
- **Mise à niveau du micrologiciel du routeur**

Statut du routeur

Dans le menu principal, sous Maintenance, sélectionnez Statut du routeur pour afficher cet écran.

Vous pouvez utiliser cet écran pour consulter le statut du routeur, des statistiques ou le statut de connexion.

- Pour en savoir plus sur les champs de cet écran, consultez le *Tableau 28*.
- Consultez la section *Affichage des statistiques* à la page 151 pour en savoir plus sur les statistiques.
- Pour en savoir plus sur la connexion Internet, consultez la section *Statut de la connexion* à la page 152.

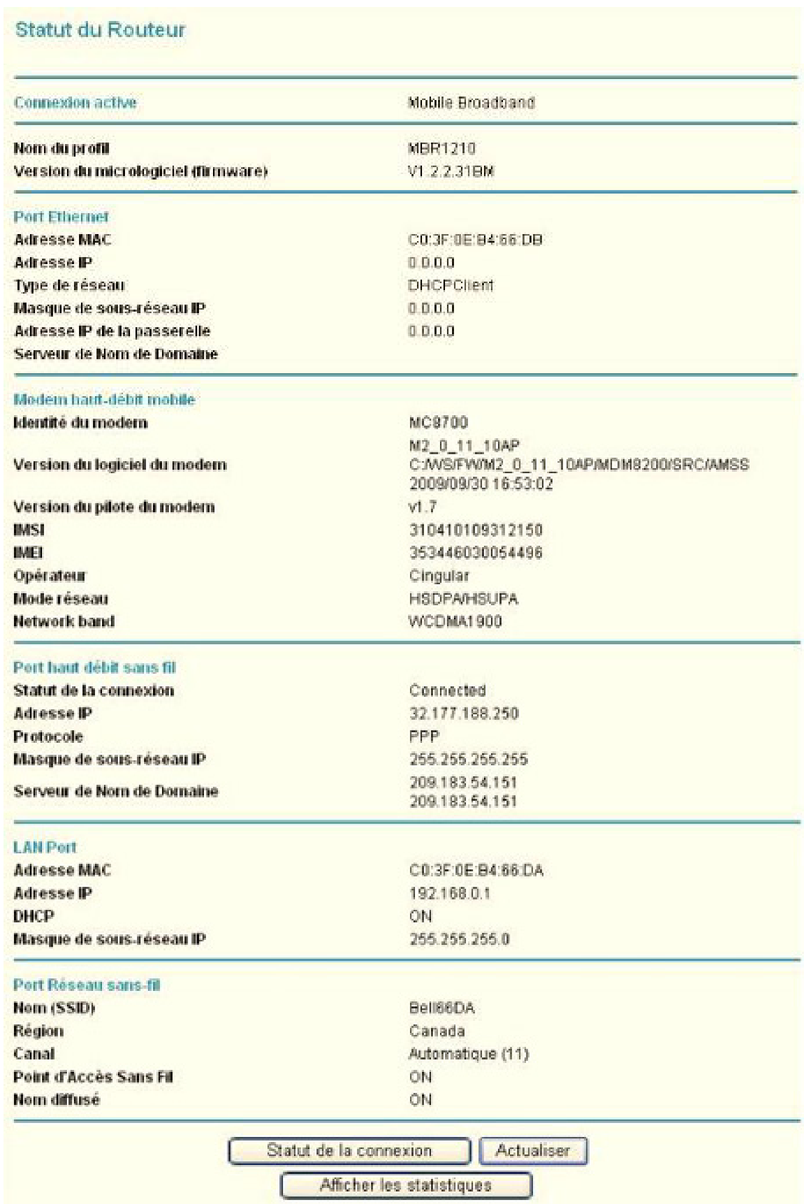
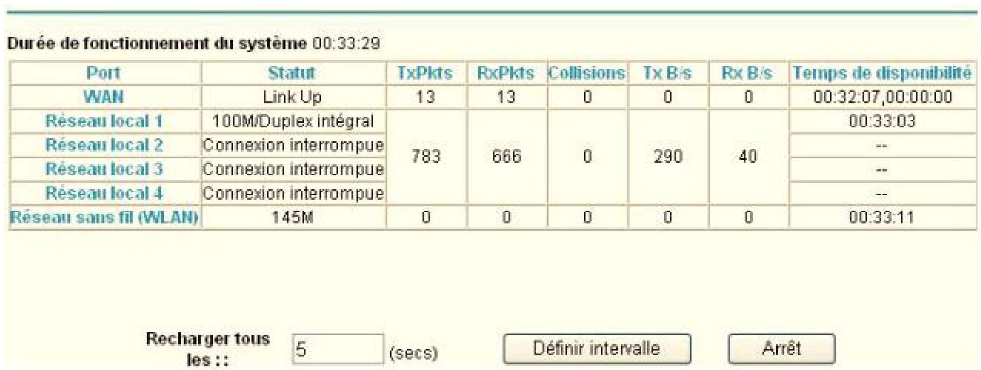


Tableau 1.

Champ		Description
Version du micrologiciel (firmware)		Ce champ affiche la version du micrologiciel du router.
Modem haut débit mobile	Identité du modem	Indique le modem utilisé.
	Version du logiciel du modem	Indique la version du logiciel du modem.
	Version du pilote du modem	Indique la version du pilote du modem.
	IMSI	International Mobile Subscriber Identity (identité internationale de l'abonné mobile). Identité de la carte SIM.
	IMEI	International Mobile Equipment Identity (identité internationale d'équipement mobile). Identité unique du modem.
	Opérateur	Fournisseur d'accès Internet pour le réseau sans fil haut débit.
	Mode réseau	Mode du réseau actuel auquel le modem est connecté. Le mode dépend de la couverture et de la distance par rapport au site cellulaire.
Port WAN	Statut de la connexion	Statut de la connexion Internet.
	Adresse IP	Adresse IP utilisée par le modem. Si aucune adresse n'est affichée, le router ne peut pas se connecter à Internet.
	Protocole	Protocole de la connexion Internet, soit PPP (protocole point à point).
	Masque de sous-réseau IP	Masque de sous-réseau IP utilisé par le port USB du router.
	Adresse IP de la passerelle	Adresse IP utilisée par le router.
	Serveur de nom de domaine	Adresses IP du serveur de nom de domaine utilisé par le router. Ces adresses sont généralement attribuées dynamiquement par le FAI.
Port LAN	MAC Address (Adresse MAC)	Adresse MAC Ethernet utilisée par le port de réseau local (LAN) du router.
	Adresse IP	Adresse IP du port de réseau local. La valeur par défaut est 192.168.0.1.
	DHCP	• **Éteint.** Le router n'attribue pas d'adresses IP aux ordinateurs du réseau local. • **Activé.** Le router attribue des adresses IP aux ordinateurs du réseau local.
	Masque de sous-réseau IP	Masque de sous-réseau IP du port de réseau local. La valeur par défaut est 255.255.255.0.
Port réseau sans fil (Consultez la section *Configuration manuelle des paramètres sans fil* à la page 129.)	Nom (SSID)	Identifiant de réseau sans fil, également appelé nom de réseau sans fil.
	Région	Pays dans lequel l'unité a été configurée à des fins d'utilisation.
	Canal	Canal actuel, lequel détermine la fréquence de fonctionnement.
	Point d'accès sans fil	Indique si la fonction de point d'accès est désactivée ou non. Si elle est désactivée, le voyant sans fil situé sur le panneau avant est éteint.
	Nom diffusé	Indique si le router est configuré de façon à diffuser son nom de réseau sans fil.

Affichage des statistiques

Cliquez sur le bouton **Afficher les statistiques**, à l'écran Statut du routeur, pour afficher les statistiques d'utilisation du router :



Durée de fonctionnement du système 00:33:29

Port	Statut	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Temps de disponibilité
WAN	Link Up	13	13	0	0	0	00:32:07,00:00:00
Réseau local 1	100M/Duplex intégral	783	666	0	290	40	00:33:03
Réseau local 2	Connexion interrompue						--
Réseau local 3	Connexion interrompue						--
Réseau local 4	Connexion interrompue						--
Réseau sans fil (WLAN)	145M	0	0	0	0	0	00:33:11

Recharger tous les :: 5 (secs) Définir intervalle Arrêt

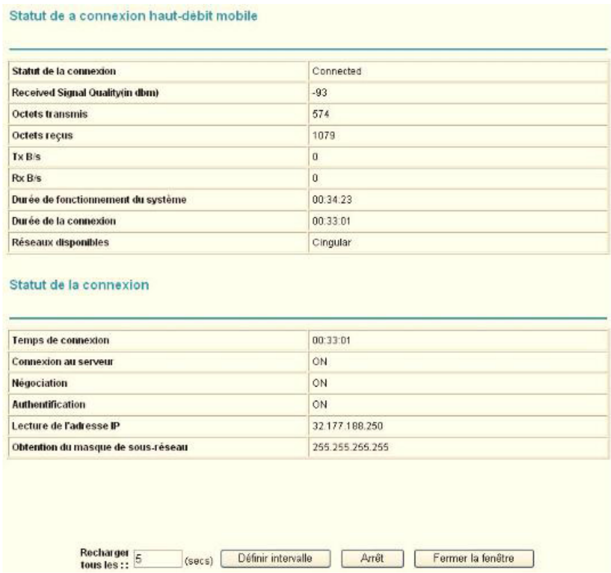
Le *Tableau 29* présente une description des champs de statistiques.

Tableau 2.

Champ	Description
Statut	Statut de la liaison. Prenez note que les réseaux locaux 2, 3 et 4 sont des réseaux d'invité.
TxPkts	Nombre de paquets transmis sur ce port depuis la dernière réinitialisation ou suppression manuelle.
RxPkts	Nombre de paquets reçus sur ce port depuis la dernière réinitialisation ou suppression manuelle.
Collisions	Nombre de collisions sur ce port depuis la dernière réinitialisation ou suppression manuelle.
Tx B/s	Utilisation moyenne de lignes de sortie pour ce port.
Rx B/s	pour ce port.
Temps de disponibilité	Temps écoulé depuis le dernier cycle d'alimentation ou réinitialisation.

Statut de la connexion

Cliquez sur le bouton **Statut de la connexion** à l'écran Statut du routeur :



Cet écran présente les statistiques suivantes :

Tableau 3.

Champ		Description
Statut de la connexion haut débit mobile	Statut de la connexion	Statut de la connexion Internet. • **Scanning** (Recherche). Le modem recherche des réseaux sans fil haut débit dans votre zone. • **Connected** (Connecté). Le router est connecté à Internet. • **No USB Device Attached** (Aucun périphérique USB connecté). Le router ne détecte aucun modem USB connecté à son port USB. Le modem est déconnecté ou incorrectement branché. Pour corriger le problème, débranchez le modem et rebranchez-le dans le port.
	Received Signal Quality (in dBm) (Qualité du signal reçu, en dBm)	Réception radio du modem. Une valeur faible ou négative indique que la qualité du signal est bonne.
	Octets transmis	Nombre d'octets transmis au cours de la dernière session de connexion.
	Octets reçus	Nombre d'octets reçus au cours de la dernière session de connexion.
	Tx B/s	Débit de transmission.
	Rx B/s	Débit de réception.
	Durée de fonctionnement du système	Temps écoulé depuis le dernier redémarrage.

Tableau 8

Champ		Description
Statut de la connexion	Temps de connexion	Temps écoulé depuis la dernière connexion à Internet via le port haut débit.
	Connexion au serveur	Statut de la connexion.
	Négociation	Réussite ou échec.
	Authentification	Réussite ou échec.
	Lecture de l'adresse IP	Adresse IP attribuée au port WAN par le fournisseur d'accès Internet ADSL.
	Obtention du masque de sous-réseau	Masque de sous-réseau attribué au port WAN par le fournisseur d'accès Internet ADSL.

Affichage des dispositifs connectés

L'écran Dispositifs connectés présente tous les dispositifs IP que le router a découvert sur le réseau local. Dans le menu principal, sous Maintenance, sélectionnez Dispositifs connectés :



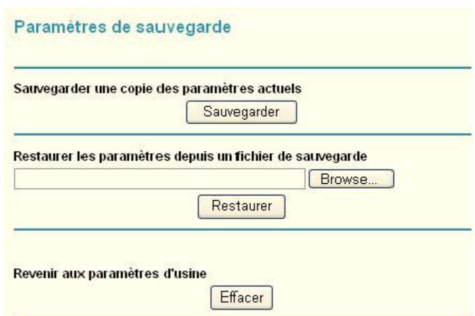
Pour chaque dispositif, le tableau présente l'adresse IP, le nom du périphérique s'il y a lieu et l'adresse MAC Ethernet. Si vous redémarrez le router, ces données sont perdues jusqu'à ce que le router redécouvre les dispositifs. Pour forcer le router à rechercher les dispositifs connectés, cliquez sur le bouton **Actualiser**.

Sauvegarde, restauration ou effacement de vos paramètres

Les paramètres de configuration du router sont conservés dans un fichier de configuration dans le router. Ce fichier peut être sauvegardé sur votre ordinateur, restauré ou rétabli aux paramètres par défaut d'usine. Les procédures des sections suivantes décrivent l'exécution de ces tâches.

Sauvegarde des paramètres de configuration dans un fichier

1. Connectez-vous au router. Tapez **http://www.routerlogin.net** dans le champ d'adresse du navigateur. Tapez **admin** pour le nom d'utilisateur et le mot de passe (ou la valeur par défaut **password**).
2. Dans le menu principal, sous Maintenance, sélectionnez Paramètres de sauvegarde pour afficher cet écran.



3. Cliquez sur **Sauvegarder** pour enregistrer une copie de vos paramètres actuels.
4. Stockez le fichier .cfg sur un ordinateur du réseau.

Restauration des paramètres de configuration à partir d'un fichier

Pour restaurer les paramètres de configuration :

1. Connectez-vous au router. Tapez **http://www.routerlogin.net** dans le champ d'adresse du navigateur. Tapez **admin** pour le nom d'utilisateur et le mot de passe (ou la valeur par défaut **password**).
2. Dans le menu principal, sous Maintenance, sélectionnez Paramètres de sauvegarde.
3. Entrez le chemin d'accès complet du fichier sur votre réseau ou cliquez sur **Browse** (Parcourir) pour rechercher le fichier.
4. Une fois le fichier .cfg trouvé, cliquez sur **Restaurer** pour charger le fichier sur le router.

   Le router redémarre.

Effacement des paramètres de configuration

Vous pouvez utiliser l'option Effacer pour supprimer les paramètres de configuration et rétablir les paramètres par défaut d'usine du router.

Pour effacer les paramètres de configuration :

1. Dans le menu principal, sous Maintenance, sélectionnez Paramètres de sauvegarde.
2. Cliquez sur **Effacer**.

   Le router redémarre.

   Après un effacement, le mot de passe du router est **password**, l'adresse IP de réseau local est **192.168.0.1** et le client DHCP du router est activé.

Remarque : Pour rétablir les paramètres par défaut d'usine lorsque vous ignorez le mot de passe de connexion ou l'adresse IP, appuyez sur le bouton de réinitialisation au bas du router pendant six secondes.

Protection de l'accès à votre Router

Pour des raisons de sécurité, le router comporte un nom d'utilisateur et un mot de passe qui lui sont propres. En outre, après une certaine période d'inactivité, la session est fermée automatiquement. Le nom d'utilisateur et le mot de passe du routeur ne sont pas les mêmes que ceux utilisés pour vous connecter à Internet.

NETGEAR recommande de remplacer ce mot de passe par un mot de passe plus sécuritaire. Le mot de passe idéal ne devrait pas figurer dans un dictionnaire, quelle que soit la langue, et il devrait comporter des lettres en majuscules et en minuscules, des chiffres et des symboles. Votre mot de passe peut comporter jusqu'à 30 caractères.

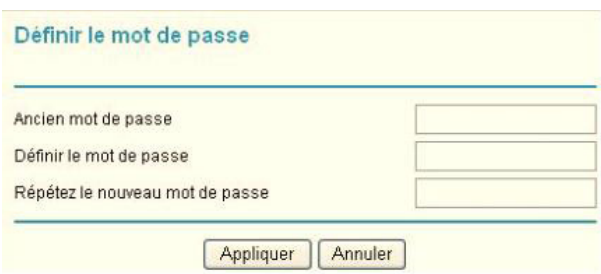
Modification du mot de passe prédéfini

1. Pour vous connecter au routeur, tapez **http://www.routerlogin.net** dans le champ d'adresse du navigateur Internet. Tapez **admin** pour le nom d'utilisateur et le mot de passe (ou la valeur par défaut **password**).

Remarque : Si vous avez changé le mot de passe et que vous ne vous en rappelez plus, vous pouvez réinitialiser les paramètres par défaut d'usine du router. Consultez la section *Rétablissement du mot de passe et de la configuration par défaut* à la page 192.

---

2. Dans le menu principal, sous Maintenance, sélectionnez Définir le mot de passe.



3. Pour changer le mot de passe, entrez l'ancien mot de passe, puis entrez deux fois le nouveau mot de passe.
4. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Remarque : Après avoir modifié le mot de passe, vous devez vous connecter de nouveau pour poursuivre la configuration. Si vous aviez sauvegardé les paramètres du router auparavant, vous devriez effectuer une nouvelle sauvegarde pour que le nouveau mot de passe soit enregistré dans le fichier de paramètres.

Modification du délai de déconnexion d'une session d'administrateur

Pour des raisons de sécurité, la connexion d'un administrateur au router est coupée après une certaine période d'inactivité. Pour modifier le délai de déconnexion :

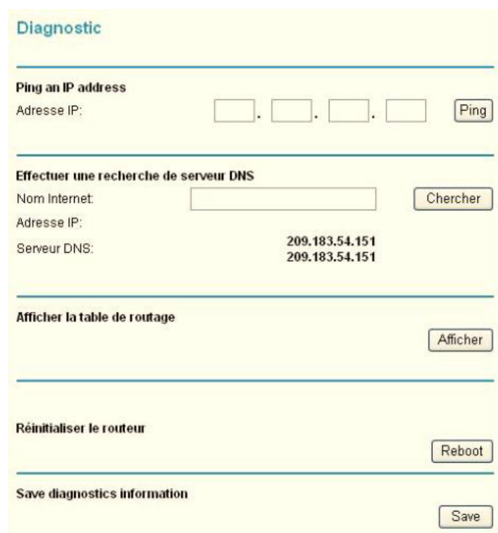
1. Dans l'écran Définir le mot de passe, tapez une valeur numérique dans le champ **Administrator login times out** (Délai de déconnexion d'une session d'administrateur). La valeur par défaut suggérée est de 5 minutes.
2. Cliquez sur **Appliquer** pour enregistrer vos modifications ou sur **Annuler** pour conserver le délai actuel.

Exécution d'utilitaires de diagnostic et redémarrage du routeur

Le router offre une fonction de diagnostic. L'écran Diagnostic vous permet d'exécuter les tâches suivantes à partir du router :

- Effectuer un Ping sur une adresse IP pour tester la connectivité afin de vérifier si vous pouvez atteindre un hôte distant. Si l'option Ping VPN est activée, le paquet ping passe toujours par le tunnel RPV si ce dernier est activé et en fonction.
- Effectuer une recherche de serveur DNS pour vérifier si un nom Internet est converti en une adresse IP, afin de s'assurer que la configuration du serveur DNS est fonctionnelle.
- Afficher la table de routage pour voir les autres routers avec lesquels votre router communique.
- Redémarrer le router pour activer des nouvelles configurations réseau ou pour supprimer des problèmes de connexion réseau avec le router.

Dans le menu principal, sous Maintenance, sélectionnez Diagnostic.



- **Ping**. Envoyer une requête Ping à une adresse IP.
- **Chercher**. Un serveur de nom de domaine (DNS) convertit un nom Internet, par exemple www.netgear.com, en une adresse IP. Si vous avez besoin de l'adresse IP d'un serveur sur Internet, vous pouvez effectuer une recherche de serveur DNS pour trouver son adresse IP.
- **Afficher**. Permet d'afficher la table de routage interne. En général, ces renseignements ne sont utilisés que par le service de soutien technique.
- **Reboot** (Redémarrer). Arrête et redémarre le routeur.

  Si vous redémarrez le routeur, vous perdez votre connexion. Pour accéder au routeur, vous devez vous y connecter de nouveau après le redémarrage.
- **Save** (Enregistrer). Enregistre les données de diagnostic.

Mise à niveau du micrologiciel du routeur

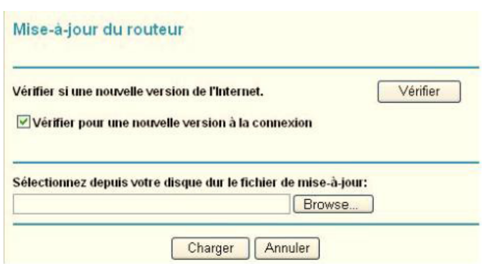
Le micrologiciel du router est stocké dans une mémoire flash et il est possible de le mettre à niveau lorsqu'une nouvelle version est offerte par NETGEAR. Les fichiers de mise à niveau peuvent être téléchargés depuis le site Web de NETGEAR. Si un fichier de mise à niveau est compressé (fichier .zip), vous devez d'abord extraire le fichier binaire (.bin ou .img) avant de le charger sur le router.

NETGEAR vous recommande d'effectuer une sauvegarde de votre configuration avant de mettre à niveau le micrologiciel. Une fois la mise à niveau terminée, il pourrait s'avérer nécessaire de rétablir vos paramètres de configuration.

1. Téléchargez et dézippez le nouveau fichier du micrologiciel depuis le site Web de NETGEAR.

   Le navigateur Web utilisé pour le chargement du fichier de micrologiciel dans le router doit prendre en charge le protocole HTTP. NETGEAR recommande d'utiliser Microsoft Internet Explorer 5.0 ou une version ultérieure, ou encore Mozilla Firefox 2.0 ou une version ultérieure.

2. Connectez-vous au router. Tapez **http://www.routerlogin.net** dans le champ d'adresse du navigateur. Tapez **admin** pour le nom d'utilisateur et le mot de passe (ou la valeur par défaut **password**).
3. Dans le menu principal, sous Maintenance, sélectionnez Mise à jour du routeur pour afficher cet écran.



4. Cliquez sur **Browse** (Parcourir) pour rechercher le fichier de mise à niveau binaire (.bin ou .img).
5. Cliquez sur **Charger**.

AVERTISSEMENT!

Lors du chargement du micrologiciel sur le router, n'interrompez pas le navigateur en fermant la fenêtre, en cliquant sur un lien ou en chargeant une nouvelle page. L'interruption du navigateur pourrait altérer le micrologiciel, ce qui rendrait le router inutilisable et inaccessible. Une fois le chargement terminé, le router redémarre automatiquement. Le processus de mise à niveau prend environ une minute. Dans certains cas, il faut effacer les paramètres de configuration et reconfigurer le router après la mise à niveau.

5. Avancé

5

Le présent chapitre décrit comment configurer les paramètres avancés de votre Mobile Broadband 11n Wireless Router.

- **Paramètres de carte SIM**
- **Paramètres sans fil avancés**
- **Fonction Répéteur sans fil**
- **Ouverture de port et déclenchement de port**
- **Paramètres WAN**
- **Paramétrage LAN**
- **Paramétrage QoS (Qualité de service)**
- **DNS Dynamique**
- **Utilisation de routes statiques**
- **Activation de la gestion à distance**
- **Service UPnP**
- **Mesure de trafic**

Paramètres de carte SIM

À partir du menu principal, sélectionnez Paramètres SIM pour afficher l'écran suivant :



Tableau 1.

Champ	Description
Activer ou Désactiver le code PIN	Contrôle si le code PIN sur la carte SIM sera utilisé pour se connecter au réseau.
Changer le Code PIN	Change le code PIN sur la carte SIM.
Statut SIM	État d'accès à la carte SIM courant.

Paramètres sans fil avancés

À partir du menu principal, sélectionnez Paramètres sans fil avancés pour afficher l'écran suivant :

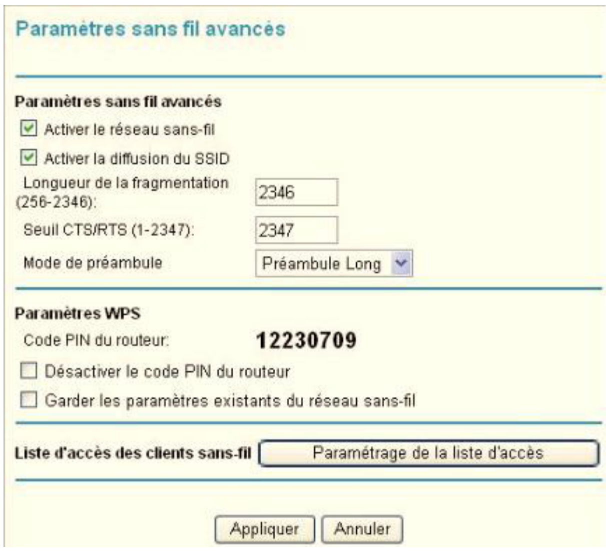


Tableau 2.

Champ	Description
Activer le réseau sans fil	Sélectionné par défaut, ce paramètre active la fréquence, qui permet au router de fonctionner comme un point d'accès sans fil. Éteindre la fréquence peut être utile pour la configuration, la mise au point du réseau ou le dépannage.
Longueur de la fragmentation, Seuil CTS/RTS et Mode de préambule	Ces paramètres devraient demeurer à leurs valeurs par défaut.
Code PIN du routeur	Le code PIN est utilisé pour la fonctionnalité « Appuyez : vous êtes connecté ».
Désactiver le code PIN du routeur	Par défaut, cette case n'est pas cochée. Cela permet aux clients WPS de découvrir le code PIN du routeur.
Garder les paramètres existants du réseau sans fil	Par défaut, cette case n'est pas cochée. Cette option permet au router de générer automatiquement le SSID et les paramètres de sécurité WPA/WPA2 lorsque WPS est pris en charge. Lorsque WPS est pris en charge, le router coche automatiquement la case **Garder les paramètres existants du réseau sans fil** pour que le SSID et les paramètres de sécurité soient conservés si d'autres périphériques prenant en charge WPS sont ajoutés ultérieurement.
Activer le contrôle d'accès	Le contrôle d'accès est désactivé par défaut, ce qui permet à tout ordinateur configuré avec le SSID correct de se connecter. Consultez la section *Restriction de l'accès par adresse MAC* à la page 163.

Contrôle d'accès de la station sans fil

Par défaut, tout PC sans fil configuré avec le SSID et les paramètres de sécurité sans fil corrects peut accéder au réseau sans fil. Il est possible d'utiliser les paramètres du point d'accès sans fil dans l'écran Paramètres sans fil avancés pour restreindre encore plus l'accès à votre réseau :

- **Désactiver complètement la connectivité sans fil**.
  Vous pouvez désactiver complètement la portion sans fil du router. Par exemple, si vous utilisez votre ordinateur portatif pour vous connecter sans fil à votre router et partez en voyage d'affaires, vous pouvez désactiver la portion sans fil du router pendant votre voyage. Les autres membres de votre famille utilisant leur ordinateur pour se connecter au router à l'aide de câbles Ethernet pourront toujours utiliser le router. Pour ce faire, décochez la case **Activer le réseau sans-fil** de l'écran Paramètres sans fil avancés, puis cliquez sur **Appliquer**.
- **Cacher le nom du réseau sans fil (SSID)**.
  Par défaut, le router est configuré pour diffuser le nom de son réseau sans fil (SSID). Vous pouvez restreindre l'accès sans fil à votre réseau en ne diffusant pas le nom du réseau sans fil (SSID). Pour ce faire, décochez la case **Activer la diffusion du SSID** dans l'écran Paramètres sans fil avancés, puis cliquez sur **Appliquer**. Les périphériques sans fil ne pourront plus « voir » votre router. Les paramètres réseau de votre périphérique sans fil doivent correspondre au nom de réseau sans fil (SSID) du router.

Remarque : Le nom de réseau de chaque adaptateur d'accès sans fil doit correspondre à celui que vous configurez dans le router. S'ils ne correspondent pas, vous ne pouvez pas établir de connexion sans fil au router.

Restriction de l'accès par adresse MAC

Pour augmenter la sécurité, vous pouvez restreindre l'accès au réseau sans fil pour n'autoriser que certains PC, en fonction de leur adresse MAC. Vous pouvez restreindre l'accès au Mobile Broadband 11n Wireless Router de manière à bloquer les PC inconnus et à n'autoriser que les PC de confiance. Le filtrage d'adresse MAC ajoute un obstacle contre les accès non autorisés à votre réseau, mais les données diffusées sur la liaison sans fil ne sont pas protégées.

Remarque : Si vous configurez le router à partir d'un ordinateur avec une connexion sans fil, ajoutez l'adresse MAC de votre ordinateur à la liste de contrôle d'accès. Autrement, vous perdrez votre connexion sans fil en cliquant sur **Appliquer**. Vous devrez ensuite accéder au router à partir d'un ordinateur avec connexion câblée ou à partir d'un ordinateur dont l'adresse MAC est dans la liste de contrôle d'accès pour effectuer des modifications.

Pour restreindre l'accès en fonction de l'adresse MAC :

1. Depuis le menu principal, sous Avancé, sélectionnez Paramètres du réseau sans fil. Cliquez sur **Paramétrage de la liste d'accès** pour afficher l'écran Liste d'accès des clients sans-fil.



2. Cochez la case **Activer le contrôle d'accès**. Ajustez la liste selon les besoins de votre réseau. Vous pouvez ajouter des périphériques à la liste de stations sans fil de confiance. Cliquez sur **Ajouter** pour afficher l'écran suivant :



3. Vous pouvez ajouter des périphériques à la liste en utilisant l'une des méthodes suivantes :
   - Si l'ordinateur est dans le tableau des cartes sans fil disponibles, sélectionnez sa case d'option pour choisir son adresse MAC.
   - Utilisez les champs d'entrée de données de carte sans fil pour entrer manuellement l'adresse MAC du périphérique souhaité. L'adresse MAC est généralement indiquée sous l'appareil sans fil.
   - Si aucun nom de périphérique n'apparaît lorsque vous entrez l'adresse MAC, vous pouvez entrer un nom décrivant l'ordinateur que vous ajoutez.
4. Cliquez sur **Appliquer** pour enregistrer ces paramètres. Maintenant, seuls les périphériques de cette liste seront autorisés à se connecter au router.

Fonction Répéteur sans fil

À partir du menu principal, sélectionnez Fonction répéteur de réseau sans fil pour afficher l'écran suivant :

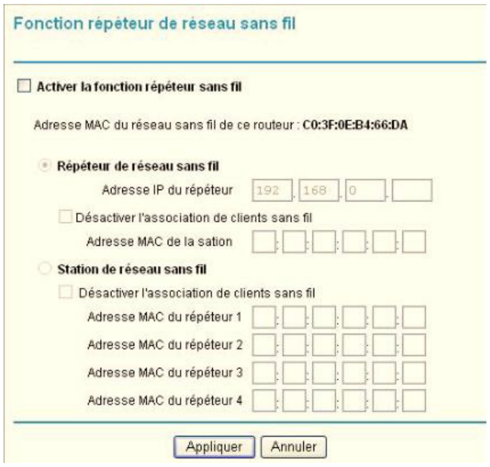


Tableau 3.

Champ	Description
Activer la fonction répéteur sans fil	Activez cette fonction si vous souhaitez utiliser le mode Pont ou Répéteur, puis sélectionnez le mode approprié pour votre environnement réseau. • **Répéteur de réseau sans fil** . Dans ce mode, le MBR1210 communique *uniquement* avec une autre station en mode Station de réseau sans fil. Vous devez entrer l'adresse MAC (adresse physique) de l'autre Station de réseau sans fil dans le champ indiqué. WEP / WPA-PSK [TKIP] peut (et devrait) être utilisé pour protéger cette communication. • **Station de réseau sans fil**. Sélectionnez cette option uniquement si ce MBR1210 est le « maître » pour un groupe de stations sans fil en mode Répéteur de réseau sans fil. Les autres stations en mode Répéteur doivent être configurées en mode Répéteur de réseau sans fil et utiliser l'adresse MAC de ce MBR1210. Elles transmettront ensuite tout leur trafic vers ce « maître » et ne communiqueront pas entre elles. WEP / WPA-PSK [TKIP] peut (et devrait) être utilisé pour protéger ce trafic. Si cette option est sélectionnée, vous devez entrer l'adresse MAC des autres points d'accès dans les champs indiqués.

Ouverture de port et déclenchement de port

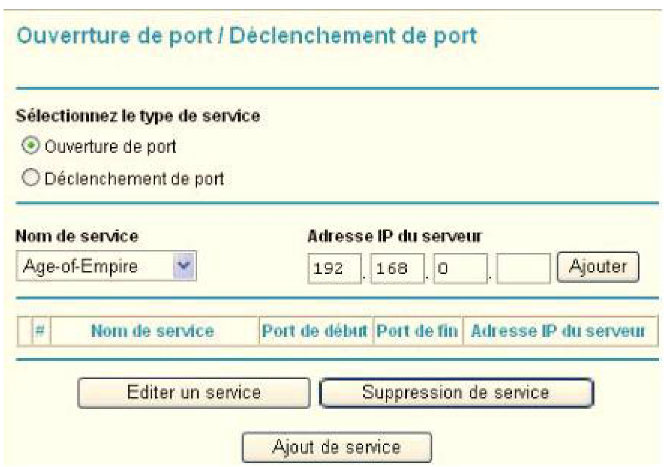
L'ouverture de port et le déclenchement de port sont des fonctions avancées qui affectent le comportement du pare-feu de votre router. Dans l'écran Ouverture de port / Déclenchement de port, vous pouvez rendre des serveurs ou des ordinateurs locaux disponibles sur Internet pour offrir divers services (par exemple, FTP ou HTTP), pour jouer à des jeux Internet (comme Quake III) ou pour utiliser des applications Internet (comme CU-SeeMe).

- L'ouverture de port est conçue pour des services Web tels FTP et les serveurs Web. Lorsque l'ouverture de port est configurée, des requêtes en provenance d'Internet sont transmises au serveur approprié.
- Le déclenchement de port surveille le trafic sortant. Lorsque le routeur détecte du trafic sur le port portant indiqué, il se souvient de l'adresse IP de l'ordinateur ayant transmis les données et déclenche le port entrant. Le trafic entrant par le port déclenché est ensuite transmis à l'ordinateur d'origine. Le déclenchement de port permet le passage des requêtes provenant d'Internet uniquement après que le port indiqué a été déclenché. Le déclenchement de port s'applique aux logiciels de clavardage et aux jeux par Internet.

Ouverture de port

Pour configurer une ouverture de port :

1. Dans le menu principal, sous Avancé, sélectionnez Ouverture de port / Déclenchement de port. L'écran suivant s'affiche :



   Par défaut, la case d'option **Ouverture de port** est sélectionnée.

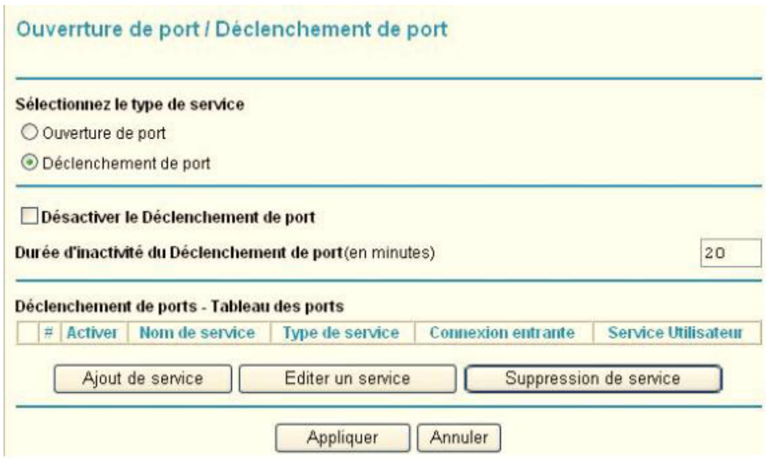
2. Vous pouvez sélectionner un service existant ou créer un service personnalisé.
   - Sélectionnez un service dans la liste déroulante **Nom de service** et entrez l'adresse IP de l'ordinateur.
   - Si vous souhaitez ajouter un service ne faisant pas partie de la liste, cliquez sur le bouton **Ajout de service**. Remplissez les champs dans l'écran Ajout de service.

   Le service apparaît dans la liste.

Déclenchement de port

Pour configurer un déclenchement de port :

1. Dans le menu principal, sous Avancé, sélectionnez Ouverture de port / Déclenchement de port.
2. Sélectionnez la case d'option **Déclenchement de port** pour afficher l'écran suivant :



3. Cliquez sur **Ajout de service** et remplissez les champs dans l'écran Ajout de service.

   Le service apparaît dans la liste. Pour de plus amples informations, consultez l'aide sous la rubrique Ouverture de port / Déclenchement de port.

Paramètres WAN

Pour modifier les paramètres de la connexion Internet haut débit, utilisez l'écran Paramètres haut débit, tel que décrit dans *Configuration manuelle de vos paramètres Internet* à la page 116.

Pour afficher ou modifier les paramètres WAN :



1. À partir du menu principal, sélectionnez Paramétrage WAN pour afficher l'écran Paramétrage WAN.
2. Effectuez les modifications voulues, puis cliquez sur **Appliquer** pour enregistrer les paramètres.

Les champs Paramètres WAN sont décrits dans le tableau ci-dessous.

Tableau 4.

Paramètre	Description
Désactiver la protection DoS et le scan de ports	Habituellement, cette case n'est pas cochée, ce qui fait en sorte que le pare-feu protège votre réseau local contre les attaques de balayage de port et de déni de service. Cette case ne devrait être cochée que dans des circonstances exceptionnelles.
Serveur DMZ par défaut	Cette fonction est parfois utile lorsque vous utilisez certains jeux et des applications de vidéoconférence en ligne. Soyez prudent lors de l'utilisation de cette fonction, parce qu'elle diminue la sécurité du pare-feu. Consultez la section *Configuration d'un serveur DMZ par défaut* à la page 169.
Répondre au ping sur le port internet	Si vous souhaitez que le router réponde à un « ping » provenant de l'Internet, cochez cette case. Cette fonction devrait être utilisée comme outil de diagnostic, puisqu'elle permet de découvrir votre router. Ne cochez pas cette case, sauf si vous avez des raisons spécifiques de le faire.
Unité de transfert maximale (MTU)	Taille de la MTU (en octets) Pour la plupart des réseaux Ethernet, la taille de la MTU est de 1500 octets, 1492 octets pour les connexions PPPoE ou 1436 octets pour les connexions PPTP.
Filtrage NAT	Il est réglé à **Sécurisé** afin de fournir un pare-feu sécuritaire, pour protéger les ordinateurs du réseau local contre les attaques provenant d'Internet. Le réglage Ouvert est moins sécuritaire.
Désactiver le SIP ALG	Certaines applications VoIP ne fonctionnent pas bien avec le SIP ALG. Cocher cette case peut aider vos périphériques VoIP à effectuer ou à accepter un appel à l'aide du router.

Configuration d'un serveur DMZ par défaut

AVERTISSEMENT!

Pour des raisons de sécurité, vous devriez éviter d'utiliser la fonction de serveur DMZ par défaut. Lorsqu'un ordinateur est désigné comme serveur DMZ par défaut, il perd presque toute la protection offerte par le pare-feu et est exposé à des exploits émanant de l'Internet. Si sa sécurité est compromise, l'ordinateur peut être utilisé pour attaquer votre réseau.

Le serveur DMZ par défaut est utile lorsque vous utilisez certains jeux et certaines applications de vidéoconférence en ligne, qui ne sont pas compatibles avec NAT. Le router est programmé pour reconnaître certaines de ces applications et pour travailler correctement avec celles-ci, mais d'autres applications pourraient ne pas fonctionner correctement. Dans certains cas, un ordinateur local peut exécuter l'application correctement si l'adresse IP de cet ordinateur est entrée comme adresse du serveur DMZ par défaut.

Le trafic entrant provenant d'Internet est habituellement ignoré par le router, sauf si le trafic est une réponse destinée à un ordinateur local ou si vous avez configuré un service dans l'écran Ports. Plutôt que d'ignorer le trafic, vous pouvez le faire suivre vers un ordinateur du réseau local. Cet ordinateur est appelé le « serveur DMZ par défaut ».

Pour définir un ordinateur ou un serveur comme serveur DMZ par défaut :

1. Ouvrez l'écran Paramètres WAN en suivant les directives de la section précédente.
2. Sélectionnez la case **Serveur DMZ par défaut**.
3. Entrez l'adresse IP de ce serveur.
4. Cliquez sur **Appliquer** pour enregistrer les modifications apportées.

Paramétrage LAN

L'écran Paramétrage LAN permet la configuration de services IP en réseau local, DHCP et RIP. Ces fonctions se trouvent sous la rubrique Avancé, dans le menu principal du router.

Le router est préconfiguré en usine afin d'utiliser les adresses IP privées du côté du réseau local et d'agir en tant que serveur DHCP. La configuration IP du LAN par défaut du router est :

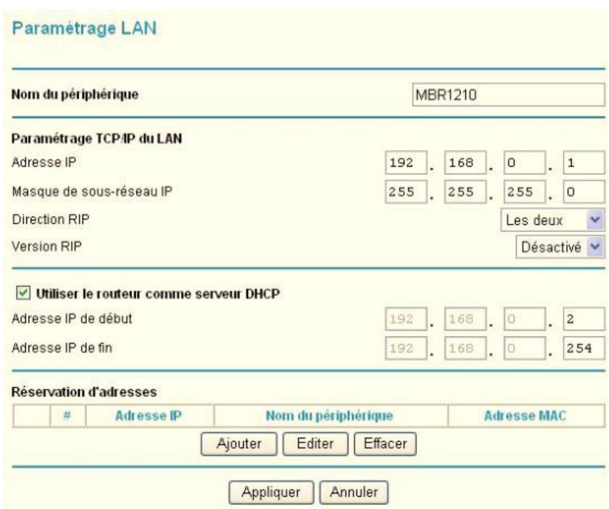
- Adresse IP du LAN : 192.168.0.1
- Masque de sous-réseau : 255.255.255.0

Ces adresses font partie de la plage d'adresses définie par le groupe de travail IETF pour les réseaux privés et devrait convenir à la plupart des applications. Si votre réseau doit utiliser un schéma d'adressage IP différent, vous pouvez effectuer des modifications dans cet écran.

> **Conseil :** Si vous modifiez l'adresse IP réseau du router à l'aide d'un navigateur Web, vous perdrez votre connexion, tout comme les autres utilisateurs connectés au router. Pour vous reconnecter au router, vous devrez ouvrir une connexion à la nouvelle adresse IP et ouvrir une nouvelle session. Il est nécessaire de redémarrer les autres ordinateurs utilisant le router pour qu'ils puissent se reconnecter au router.

Pour afficher ou modifier le paramétrage LAN :

1. Sélectionnez IP du réseau local pour afficher l'écran Paramétrage LAN.



2. Modifiez les paramètres. Pour obtenir plus d'information, consultez *Paramètres de serveur DHCP* à la page 171 ou *Réservation d'adresses* à la page 172.
3. Cliquez sur **Appliquer** pour enregistrer vos modifications.

Les paramètres Paramétrage TCP/IP du LAN sont expliqués dans le tableau ci-dessous.

Tableau 5.

Paramètres		Description
Nom du périphérique		
Paramétrage TCP/IP du LAN	Adresse IP	L'adresse IP du réseau local du router.
	Masque de sous-réseau IP	Le masque de sous-réseau du réseau local du router. Lorsque combiné à une adresse IP, le masque de sous-réseau IP permet à un périphérique de savoir quelles adresses sont locales et quelles adresses doivent être atteintes à l'aide d'une passerelle ou du router.
Serveur DHCP Pour obtenir plus d'information, consultez la section *Paramètres de serveur DHCP* à la page 171.	Utiliser le routeur comme serveur DHCP	Cette case est habituellement cochée, ce qui permet au router de fonctionner comme serveur DHCP. Consultez la section *Paramètres de serveur DHCP* à la page 171.
	Adresse IP de début	Définit le début de la plage définie comme réserve d'adresses IP dans le même sous-réseau que le router.
	Adresse IP de fin	Définit la fin de la plage définie comme réserve d'adresses IP dans le même sous-réseau que le router.
Réservation d'adresses Pour obtenir plus d'information, consultez la section *Paramètres de serveur DHCP* à la page 171.		Lorsque vous définissez une adresse IP réservée pour un ordinateur du réseau local, cet ordinateur se fait attribuer la même adresse IP chaque fois qu'il reçoit une adresse du serveur DHCP du routeur. Attribuez des adresses IP réservées à des serveurs nécessitant des paramètres IP permanents.

Paramètres de serveur DHCP

Par défaut, le router fonctionne comme un serveur DHCP, ce qui lui permet d'attribuer les adresses IP, l'adresse du serveur DNS et l'adresse de la passerelle par défaut à tous les ordinateurs connectés au réseau local du router. L'adresse de passerelle par défaut assignée est l'adresse du LAN du router. Les adresses IP sont attribuées aux PC connectés au réseau local à partir de la réserve d'adresses définie dans cet écran. Chaque adresse de la réserve est testée avant l'attribution, pour éviter de dupliquer les adresses dans le réseau local.

Pour la plupart des applications, les paramètres par défaut DHCP et TCP/IP définis dans le router sont adéquats. Cliquez sur le lien vers le document en ligne *Principes de base d'un réseau ITCP/IP* à la page 197 pour obtenir des explications sur DHCP et des informations sur l'attribution des adresses IP pour votre réseau local.

Utiliser le routeur comme serveur DHCP

Si un autre périphérique connecté à votre réseau agit en tant que serveur DHCP ou si vous préférez configurer manuellement les paramètres réseau de tous vos ordinateurs, décochez la case **Utiliser le routeur comme serveur DHCP** dans l'écran Paramétrage LAN. Autrement, laissez cette case cochée.

Définissez la réserve d'adresses IP pouvant être attribuées en remplissant les champs **Adresse IP de début** et **Adresse IP de fin**. Ces adresses devraient faire partie du même sous-réseau que l'adresse IP du router. Avec le schéma d'adressage par défaut, vous devriez définir une plage entre 192.168.0.2 et 192.168.0.254, en réservant peut-être une partie de cette plage pour les périphériques ayant une adresse fixe.

Le router fournit les paramètres suivants à tous les périphériques du réseau local transmettant une requête DHCP :

- Une adresse IP provenant de la plage que vous avez définie.
- Masque de sous-réseau :
- L'adresse IP de la passerelle est l'adresse IP du routeur dans le réseau local.
- Le serveur DNS principal, si vous avez entré une adresse DNS principale dans l'écran Paramètres de base; sinon, l'adresse IP du routeur dans le réseau local.
- Le serveur DNS secondaire, si vous avez entré une adresse DNS secondaire dans l'écran Paramètres de base.
- Le serveur WINS (Windows Internet Naming Service) détermine l'adresse IP associée à un ordinateur Windows donné. Un serveur WINS enregistre et fournit une liste des noms et adresses IP des PC roulant sous Windows dans le réseau local. Si vous vous connectez à un réseau distant contenant un serveur WINS, entrez l'adresse IP du serveur ici. Cela permet à vos PC de parcourir le réseau en utilisant la fonction Network Neighborhood de Windows.

Réservation d'adresses

Lorsque vous définissez une adresse IP fixe pour un ordinateur dans votre réseau local, cet ordinateur se voit attribuer la même adresse IP chaque fois qu'il accède au serveur DHCP du router. Les adresses IP réservées devraient être attribuées à des serveurs ayant besoin de paramètres IP permanents.

Pour réserver une adresse IP :

1. Cliquez sur le bouton **Ajouter**.
2. Dans le champ **Adresse IP**, entrez l'adresse IP fixe attribuée à l'ordinateur ou au serveur. Choisissez une adresse IP faisant partie du sous-réseau du réseau local du routeur, par exemple 192.168.0.x.
3. Entrez l'adresse MAC de l'ordinateur ou du serveur.

   Conseil : Si l'ordinateur ou le serveur se trouve dans votre réseau, il apparaît dans le même écran, pour vous simplifier la vie. Lorsque vous cliquez sur la case d'option de chaque périphérique dans la liste, les champs d'adresse MAC et de nom sont remplis automatiquement.

4. Cliquez sur **Appliquer** pour entrer l'adresse réservée dans le tableau.

Remarque : L'adresse réservée ne sera pas attribuée jusqu'à ce que cet ordinateur communique avec le serveur DHCP. Redémarrez l'ordinateur ou ouvrez sa configuration IP et forcez l'abandon et le renouvellement de l'adresse IP avec DHCP.

Pour modifier ou supprimer une entrée d'adresse réservée :

1. Cliquez sur le bouton à côté de l'adresse réservée que vous souhaitez modifier ou supprimer.
2. Cliquez sur **Éditer** ou **Effacer**.

Paramétrage QoS (Qualité de service)

QoS est une fonction avancée pouvant être utilisée pour définir la priorité de certaines applications Internet et de jeux en ligne, minimisant l'impact lorsque la bande passante est très sollicitée.

À partir du menu principal, sélectionnez Paramétrage QoS pour afficher l'écran suivant :

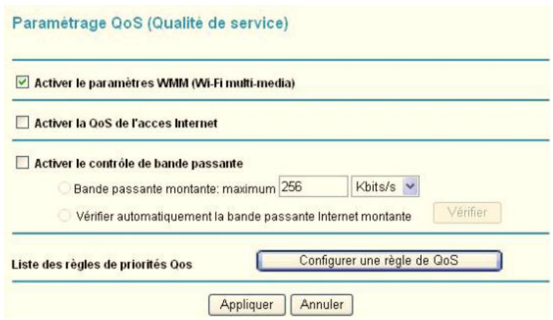
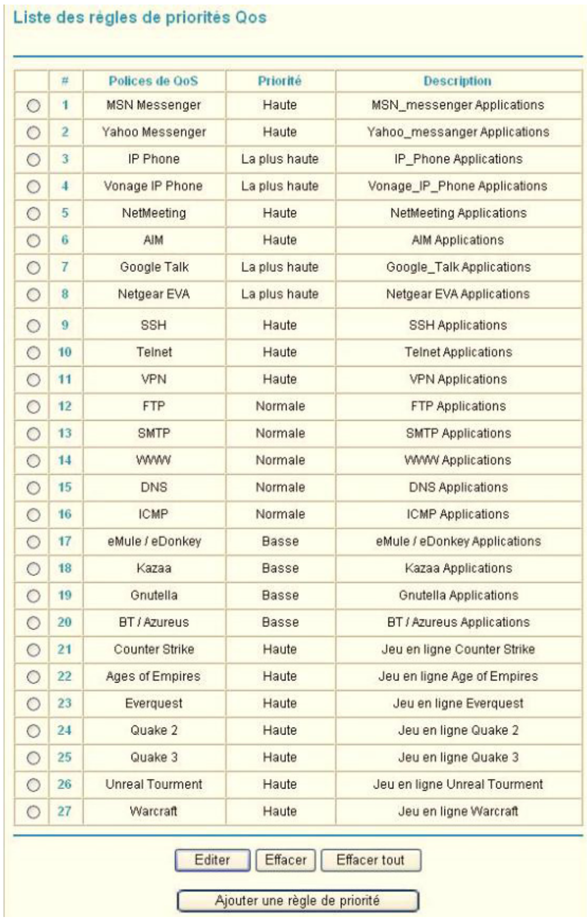


Tableau 6.

Champ	Description
Activer les paramètres WMM (Wi-Fi Multi-media)	WMM (Wireless Multimedia) est un sous-ensemble du standard 802.11e. WMM permet de définir une large gamme de priorités, en fonction des données transmises à l'aide de la connexion sans fil. Les données affectées par les délais, comme la vidéo et l'audio, obtiennent une priorité plus élevée que le trafic normal. Pour que WMM fonctionne correctement, les clients sans fil doivent aussi prendre en charge WMM.
Activer la QoS de l'accès Internet	Si vous activez QoS, la fonction QoS établit la priorité du trafic d'accès à Internet. Pour les applications déjà définies dans la liste déroulante (par exemple, Jeu en ligne, Ethernet LAN Port ou une adresse MAC définie), vous pouvez modifier le niveau de priorité en cliquant sur le bouton **Éditer** ou encore, cliquez sur **Effacer** pour supprimer la règle de priorité. Vous pouvez aussi définir des politiques de priorité pour des jeux en ligne, des applications, un port LAN ou l'adresse MAC de l'ordinateur, en cliquant sur le bouton **Ajouter une règle de priorité**.
Activer le contrôle de bande passante	Pour configurer la bande passante maximale totale pour la liaison ascendante, cliquez sur le bouton **Vérifier** pour détecter la bande passante actuelle, ce qui vous aidera à déterminer le réglage maximal.

Liste des règles de priorités QoS

Dans l'écran Paramétrage QoS, cliquez sur **Configurer une règle de QoS** pour afficher l'écran suivant :



Liste des règles de priorités Qos

	#	Polices de QoS	Priorité	Description
○	1	MSN Messenger	Haute	MSN_messenger Applications
○	2	Yahoo Messenger	Haute	Yahoo_messanger Applications
○	3	IP Phone	La plus haute	IP_Phone Applications
○	4	Vonage IP Phone	La plus haute	Vonage_IP_Phone Applications
○	5	NetMeeting	Haute	NetMeeting Applications
○	6	AIM	Haute	AIM Applications
○	7	Google Talk	La plus haute	Google_Talk Applications
○	8	Netgear EVA	La plus haute	Netgear EVA Applications
○	9	SSH	Haute	SSH Applications
○	10	Telnet	Haute	Telnet Applications
○	11	VPN	Haute	VPN Applications
○	12	FTP	Normale	FTP Applications
○	13	SMTP	Normale	SMTP Applications
○	14	WWW	Normale	WWW Applications
○	15	DNS	Normale	DNS Applications
○	16	ICMP	Normale	ICMP Applications
○	17	eMule / eDonkey	Basse	eMule / eDonkey Applications
○	18	Kazaa	Basse	Kazaa Applications
○	19	Gnutella	Basse	Gnutella Applications
○	20	BT / Azureus	Basse	BT / Azureus Applications
○	21	Counter Strike	Haute	Jeu en ligne Counter Strike
○	22	Ages of Empires	Haute	Jeu en ligne Age of Empires
○	23	Everquest	Haute	Jeu en ligne Everquest
○	24	Quake 2	Haute	Jeu en ligne Quake 2
○	25	Quake 3	Haute	Jeu en ligne Quake 3
○	26	Unreal Tourment	Haute	Jeu en ligne Unreal Tourment
○	27	Warcraft	Haute	Jeu en ligne Warcraft

Editer | Effacer | Effacer tout

Ajouter une règle de priorité

QoS - Règles de priorité

À partir de la Liste des règles de priorités QoS, cliquez sur **Ajouter une règle de priorité** pour afficher l'écran suivant :



Pour Applications ou Jeu en ligne

Pour paramétrer la priorité d'une application ou d'un jeu en ligne :

1. Sélectionnez **Applications** ou **Jeu en ligne** dans les listes **Catégorie de priorité**.



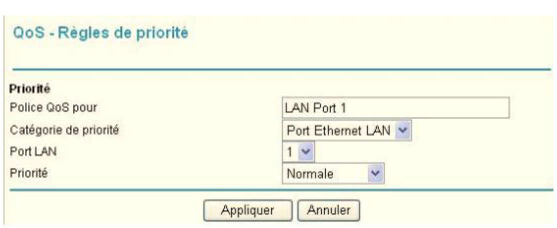


2. Sélectionnez l'application ou le jeu Internet pour lequel vous souhaitez définir la priorité à partir de la liste pertinente.
3. Sélectionnez le niveau de priorité : **Le plus élevé**, **Élevé**, **Normal** ou **Bas**.
4. Vous pouvez également entrer le nom dans le champ **Police QoS pour** pour cette règle, si vous le désirez.
5. Cliquez sur **Appliquer**.

Pour Port Ethernet LAN

Pour configurer la priorité de port LAN :

1. Sélectionnez **Port Ethernet LAN** dans la liste **Catégorie de priorité**.



2. Sélectionnez le numéro de port LAN pour lequel vous souhaitez définir le niveau de priorité, pour les ordinateurs se connectant à ce port LAN.
3. Sélectionnez le niveau de priorité : **Le plus élevé**, **Élevé**, **Normal** ou **Bas**.
4. Vous pouvez également entrer le nom dans le champ **Police QoS pour** pour cette règle, si vous le désirez.
5. Cliquez sur **Appliquer**.

Pour les adresses MAC

Pour configurer la priorité à l'ordinateur spécifié par le biais de son adresse MAC :

1. Sélectionnez **Adresse MAC** dans la liste **Catégorie de priorité**.



2. Cliquez sur le bouton **Actualiser** pour mettre à jour la liste des ordinateurs déjà raccordés au routeur.
3. Sélectionnez la case d'option de l'entrée.
4. Modifiez l'information dans les champs **Adresse MAC** et **Nom du périphérique**.
5. Sélectionnez le niveau de priorité : **Le plus élevé**, **Élevé**, **Normal** ou **Bas**.
6. Vous pouvez également entrer le nom dans le champ **Police QoS pour** pour cette règle, si vous le désirez.
7. Cliquez sur le bouton **Éditer**.
8. Cliquez sur **Appliquer**.

Pour ajouter la priorité à l'ordinateur spécifié par le biais de son adresse MAC :

1. Sélectionnez **Adresse MAC** dans la liste **Catégorie de priorité**.
2. Entrez l'adresse MAC de l'ordinateur pour lequel vous définissez la priorité.
3. Vous pouvez aussi entrer un nom facile à mémoriser dans les champs **Nom du périphérique**.
4. Sélectionnez le niveau de priorité : **Le plus élevé**, **Élevé**, **Normal** ou **Bas**.
5. Vous pouvez également entrer un nom dans le champ **Police QoS pour** pour cette règle, si vous le désirez.
6. Cliquez sur le bouton **Ajouter**.
7. Cliquez sur **Appliquer**.

Pour supprimer une entrée de règle de priorité :

1. Sélectionnez la case d'option de l'entrée du tableau.
2. Cliquez sur le bouton **Effacer**.
3. Cliquez sur **Appliquer**.

DNS Dynamique

Si votre réseau a une adresse IP attribuée de manière permanente, vous pouvez enregistrer un nom de domaine et le lier à votre adresse IP à l'aide d'un serveur DNS public. Toutefois, si votre compte Internet utilise une adresse IP attribuée dynamiquement, vous ne connaîtrez pas à l'avance votre adresse IP et cette adresse change régulièrement. Dans ce cas, vous pouvez utiliser un service DNS dynamique commercial pour lier votre domaine à l'adresse IP et diriger le trafic destiné à votre domaine vers votre adresse IP, même si elle change fréquemment.

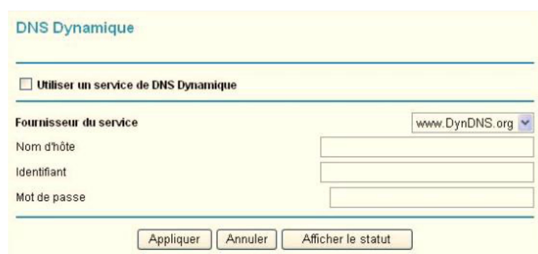
Le router contient un client pouvant se connecter à un fournisseur de service DNS dynamique. Pour utiliser cette fonction, vous devez choisir un fournisseur de service et obtenir un compte. Après avoir configuré vos informations de compte dans le router, lorsque votre adresse IP attribuée par votre FAI change, votre router communiquera automatiquement avec votre fournisseur de service DNS dynamique, ouvrira une session dans votre compte et enregistrera la nouvelle adresse IP.

AVERTISSEMENT!

Si votre FAI attribue une adresse WAN privée, comme 192.168.x.x ou 10.x.x.x, le service de DNS dynamique ne fonctionnera pas parce que les adresses privées ne sont pas acheminées sur Internet.

Pour configurer un DNS dynamique :

1. Dans le menu principal, sélectionnez **DNS Dynamique** pour afficher l'écran DNS Dynamique :



2. Accédez au site web d'un des fournisseurs de service de DNS Dynamique dont le nom apparaît dans la liste déroulante **Fournisseur du service** et inscrivez-vous pour obtenir un compte.

   Par exemple, pour dyndns.org, visitez le site www.dyndns.org.

3. Cochez la case **Utiliser un service de DNS Dynamique** .
4. Sélectionnez le nom de votre fournisseur du service de DNS Dynamique.
5. Remplissez les champs **Nom d'hôte**, **Identifiant** et **Mot de passe**.

   Le fournisseur du service de DNS Dynamique pourrait faire référence au nom d'hôte en le nommant « nom de domaine ». Si votre URL est monNom.dyndns.org, alors votre nom d'hôte est monNom. Le mot de passe peut être une clé pour votre compte DNS Dynamique.

   Si votre fournisseur de DNS Dynamique permet l'utilisation de caractères de remplacement pour la résolution de votre URL, vous pouvez sélectionner la case à cocher **Utiliser caractères de remplacement** pour activer cette fonction.

   Par exemple, la fonction de caractère de remplacement fera en sorte que *.votreserveur.dyndns.org sera traduit avec la même adresse IP que votreserveur.dyndns.org.

6. Cliquez sur **Appliquer** pour enregistrer votre configuration.

Utilisation de routes statiques

Les routes statiques fournissent des informations d'acheminement supplémentaires à votre router. Dans des circonstances normales, le router contient des informations de routage adéquates après avoir été configuré pour l'accès Internet et vous n'avez pas besoin de configurer des routes statiques supplémentaires. Vous devez configurer des routes statiques pour les cas inhabituels, par exemple lorsqu'il y a plusieurs routeurs ou plusieurs sous-réseaux IP dans votre réseau.

Exemple de route statique

Le cas suivant illustre une situation où une route statique est nécessaire :

- Votre accès Internet principal se fait à l'aide d'un modem câble, vers un FAI.
- Votre réseau domestique utilise un routeur ISDN pour se connecter à l'entreprise pour laquelle vous travaillez. L'adresse de ce routeur sur votre réseau local est 192.168.0.100.
- Le réseau de votre entreprise est 134.177.0.0.

Lorsque vous avez configuré votre routeur, deux routes statiques implicites ont été créées. Une route par défaut a été créée vers votre FAI pour le router et une seconde route statique a été créée pour votre réseau local, pour toutes les adresses 192.168.0.x. Avec cette configuration, si vous tentez d'accéder à un service sur le réseau 134.177.0.0, votre routeur achemine votre requête à votre FAI. Le FAI achemine votre requête vers votre employeur et la requête sera fort probablement bloquée par le pare-feu de l'entreprise.

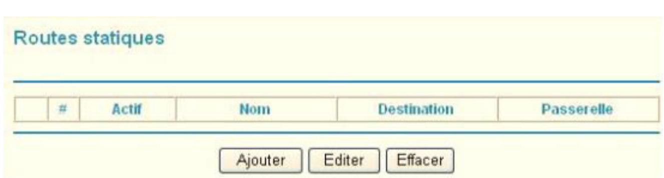
Dans ce cas, vous devez définir une route statique, en indiquant à votre routeur que 134.177.0.0 doit être accédé par le routeur ISDN à l'adresse 192.168.0.100.

Dans cet exemple :

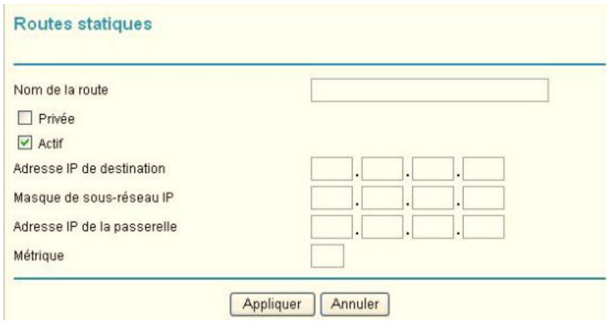
- Les champs **Adresse IP de destination** et **Masque de sous-réseau IP** spécifient que cette route statique s'applique à toutes les adresses 134.177.x.x.
- Les champs **Adresse IP de la passerelle** spécifient que tout le trafic pour ces adresses devrait être transféré vers le routeur ISDN à l'adresse 192.168.0.100.
- Dans le champ **Métrique**, une valeur de 1 fonctionnera puisque le routeur ISDN se trouve sur le réseau local.
  Cela représente le nombre de routeurs entre votre réseau et la destination. Il s'agit d'une connexion directe, il est donc configuré à 1.
- **Privée** est sélectionné uniquement par mesure de précaution, en cas d'activation de RIP.

Pour configurer des routes statiques :

1. Dans le menu principal, sous Avancé, sélectionnez Routes statiques pour afficher l'écran Routes statiques.



2. Sélectionnez la case d'option de la route statique à configurer.
3. Cliquez sur **Ajouter** ou **Éditer** pour afficher l'écran suivant :



4. Remplissez ou modifiez les champs :
   - **Nom de la route.** Ce n'est que pour des besoins d'identification.
   - **Privée**. Cochez cette case si vous désirez limiter l'accès au réseau local seulement. La route statique ne sera pas rapportée dans RIP.
   - **Actif**. Cochez cette case pour rendre cette route active.
   - **Adresse IP de destination** et **Masque de sous-réseau IP**. Si la destination est un seul hôte, entrez une valeur de sous-réseau de **255.255.255.255**.
   - **Adresse IP de la passerelle**. Cela doit être un routeur sur le même segment de réseau local que le router.
   - **Métrique**. Entrez un chiffre entre 2 et 15. Cela représente le nombre de routeurs entre votre réseau et la destination. En général, un paramètre de 2 ou 3 fonctionne, mais s'il s'agit d'une connexion directe, configurez-le à 2.
5. Cliquez sur **Appliquer** pour enregistrer les modifications apportées. Si vous avez ajouté une route statique, elle est ajoutée à l'écran Routes statiques.

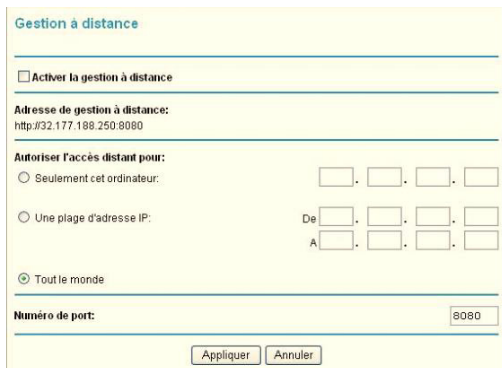
Activation de la gestion à distance

À l'aide de l'écran Gestion à distance, vous pouvez permettre aux utilisateurs sur l'Internet de configurer, de mettre à niveau et de vérifier l'état de votre router.

Conseil : Assurez-vous de modifier le mot de passe par défaut du router pour un mot de passe très sécuritaire. Le mot de passe idéal ne devrait pas contenir de mots de dictionnaire (peu importe la langue) et devrait être une combinaison de lettres (autant majuscules que minuscules), de chiffres et de symboles. Votre mot de passe peut comporter jusqu'à 30 caractères.

Pour configurer Gestion à distance

1. Connectez-vous au router. Tapez **http://www.routerlogin.net** dans le champ d'adresse du navigateur. Tapez **admin** pour le nom d'utilisateur et le mot de passe (ou la valeur par défaut **password**).
2. Sous Avancé, sélectionnez Gestion à distance :



3. Cochez la case **Activer la gestion à distance** .
4. Spécifiez les adresses externes qui permettront d'accéder à la gestion à distance du router.

   Par mesure de sécurité, restreignez l'accès au plus petit nombre d'adresses IP externes que possible :

   - Pour permettre l'accès à partir de n'importe quelle adresse IP sur l'Internet, sélectionnez **Tout le monde**.
   - Pour permettre l'accès à une plage d'adresses IP sur l'Internet, sélectionnez **Une plage d'adresse IP**. Entrez une adresse IP de début et de fin pour définir la plage permise.
   - Pour permettre l'accès à une seule adresse IP sur l'Internet, sélectionnez **Seulement cet ordinateur**.
     Entrez l'adresse IP qui permettra l'accès au réseau.
5. Spécifiez le numéro de port qui sera utilisé pour accéder au menu du routeur.

   L'accès utilise normalement le port 80 du service HTTP standard. Pour une sécurité accrue, vous pouvez entrer un numéro de port différent. Choisissez un nombre entre 1024 et 65535, mais n'utilisez pas le numéro d'un port de service commun. La valeur par défaut est 8080. Il s'agit d'un substitut courant pour HTTP.
6. Cliquez sur **Appliquer** pour que vos modifications prennent effet.

   Lorsque vous accédez à votre router de l'Internet, entrez l'adresse IP WAN de votre router dans le champ d'adresse ou d'emplacement de votre navigateur Internet, suivie de deux points (:) et du numéro de port personnalisé. Par exemple, si votre adresse externe est 134.177.0.123 et que vous utilisez le numéro de port 8080, entrez : **http://134.177.0.123:8080.** Assurez-vous d'inclure http:// dans l'adresse.

Service UPnP

L'Universal Plug and Play (UPnP) aide les périphériques tels que les ordinateurs et les appareils Internet, à accéder au réseau et à se connecter à d'autres périphériques selon les besoins. Les périphériques UPnP peuvent détecter automatiquement sur le réseau les services d'autres périphériques UPnP enregistrés.

1. Sélectionnez UPnP dans le menu principal pour afficher l'écran UPnP :

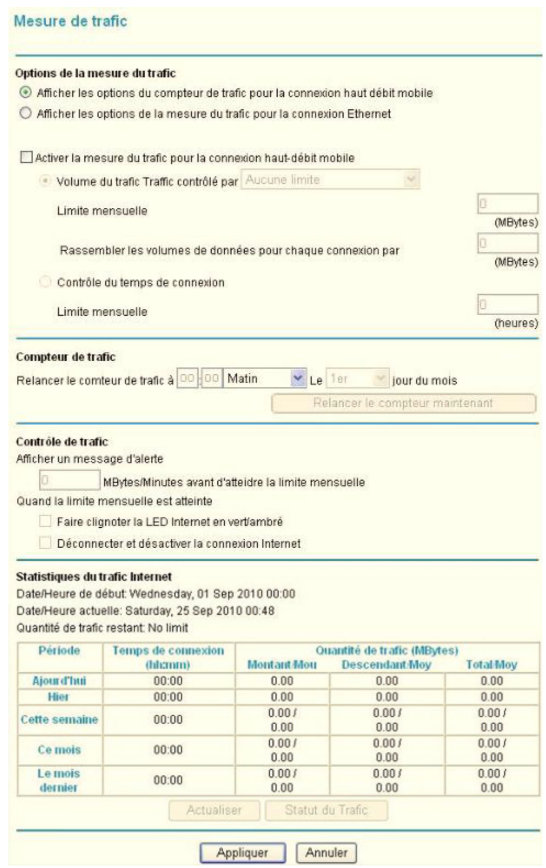


2. Remplissez les paramètres de l'écran UPnP :
   - **Activer l'UPnP**. L'UPnP peut être activé ou désactivé pour la configuration de périphérique automatique. Le paramètre par défaut pour l'UPnP est activé. Si cette fonction est désactivée, le router ne permettra à aucun périphérique de commander automatiquement les ressources, comme l'ouverture de port (mappage), du router.
   - **Intervalle de diffusion**. L'intervalle de diffusion représente la fréquence à laquelle le router diffuse ses informations UPnP. Cette valeur peut être spécifiée entre 1 et 1440 minutes. L'intervalle par défaut est de 30 minutes. Des intervalles inférieurs permettront aux points de contrôle d'obtenir l'état courant des périphériques, mais au prix d'un surcroît de trafic réseau. Des intervalles plus longs peuvent compromettre l'actualisation de l'état des périphériques mais peuvent réduire de manière significative le trafic réseau.
   - **Durée de vie de diffusion**. La durée de vie de diffusion se mesure en sauts pour chaque paquet UPnP envoyé. Un saut représente le nombre d'étapes autorisées pour la propagation de chaque diffusion UPnP avant qu'elle ne disparaisse. Le nombre de sauts peut être spécifié entre 1 et 255. La valeur par défaut de la durée de vie de diffusion est de 4 sauts, ce qui convient parfaitement à la plupart des réseaux domestiques. Si vous remarquez que certains périphériques ne sont pas correctement mis à jour ou inaccessibles, il peut alors être nécessaire d'augmenter légèrement cette valeur.
   - **Tableau des ports UPnP**. Le Tableau des ports UPnP affiche l'adresse IP de chaque périphérique UPnP qui accède présentement au router et les ports (internes et externes) que le périphérique a ouverts.
3. Pour enregistrer ou annuler vos modifications ou actualiser le tableau :
   - Cliquez sur **Appliquer** pour enregistrer les nouveaux paramètres au router.
   - Cliquez sur **Annuler** pour ignorer toute modification non enregistrée.
   - Cliquez sur **Actualiser** pour mettre à jour le tableau des ports et afficher les ports actifs qui sont présentement ouverts par les périphériques UPnP.

Mesure de trafic

Le compteur de trafic vous permet de surveiller le volume de trafic Internet qui passe par le port Internet de votre router. Grâce à l'utilitaire Compteur de trafic, vous pouvez configurer des limites pour le volume de trafic, configurer une limite mensuelle et obtenir une mise à jour en temps réel du trafic. Vous activez des compteurs de trafic distincts pour la connexion haut débit mobile et la connexion Ethernet.

Pour surveiller le trafic sur votre routeur :



1. Sous Avancé dans le menu du routeur, sélectionnez Mesure de trafic.
2. Cliquez sur la case d'option **Afficher les options du compteur de trafic pour ...** appropriée pour le type de connexion Internet (p. ex., haut débit mobile ou Ethernet) que vous configurez.
3. Pour activer le compteur de trafic, cochez la case **Activer la mesure du trafic** .
4. Si vous désirez enregistrer et restreindre le volume de trafic Internet, sélectionnez la case d'option **Volume du trafic contrôlé par** . Vous pouvez sélectionner l'une des options suivantes pour contrôler le volume de trafic :
   - **Aucune limite**. Aucune restriction n'est appliquée quand la limite de trafic est atteinte.
   - **Téléchargement uniquement**. La restriction spécifiée s'applique uniquement aux données entrantes.
   - **Dans les deux sens**. La restriction spécifiée s'applique aux données entrantes et sortantes.
5. Vous pouvez limiter la quantité de données transférées permise par mois :
   - en spécifiant le nombre de mégaoctets par mois permis;
   - en spécifiant le nombre d'heures de trafic permis.
6. Paramétrez le Compteur de trafic pour qu'il commence à une heure et une date en particulier.
7. Configurez le contrôle de trafic pour qu'il émette un message d'avertissement avant d'atteindre la limite mensuelle de mégaoctets ou d'heures. Vous pouvez sélectionner l'une des deux options suivantes quand la limite est atteinte :
   - Faire clignoter la LED Internet en vert/ambré.
   - Déconnecter et désactiver la connexion Internet.
8. Configurez **Statistiques du trafic Internet** pour surveiller le trafic de données.
9. Cliquez sur le bouton **Statut du trafic** si vous désirez une mise à jour en direct de l'état du trafic Internet sur votre routeur.
10. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

6. Dépannage

6

Ce chapitre contient des renseignements sur le dépannage de votre Mobile Broadband 11n Wireless Router. Après la description de chaque problème, des instructions sont fournies pour vous aider à établir un diagnostic et à corriger la situation. Pour les problèmes courants présentés, accédez à la section indiquée.

- Le routeur est-il sous tension?

  Consultez la section *Fonctionnement de base* à la page 185.

- Le routeur est-il correctement connecté?

  Consultez la section *Fonctionnement de base* à la page 185.

- Impossible d'accéder à la configuration du routeur à partir de mon navigateur.

  Consultez la section *Dépannage de l'accès au menu principal du routeur* à la page 187.

- J'ai configuré le routeur mais je ne parviens pas à accéder à Internet.

  Consultez la section *Dépannage de la connexion au FAI* à la page 188.

- J'aimerais effacer les données de configuration et recommencer entièrement la procédure.

  Consultez la section *Rétablissement du mot de passe et de la configuration par défaut* à la page 192.

Fonctionnement de base

Une fois que le routeur est sous tension, la séquence d'événements suivante devrait se produire :

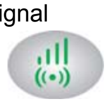
1. Après la mise sous tension initiale, vérifiez que le voyant d'alimentation  est allumé.
2. Après 10 secondes environ, vérifiez que :
   a. Le voyant d'alimentation reste allumé en vert. Un voyant orange vous indique que le test d'autodiagnostic de l'appareil a échoué.
   b. Le voyant Internet est allumé.
   c. Le voyant de liaison radio Wi-Fi est allumé. La liaison radio Wi-Fi est activée par défaut.
   d. Le voyant de port Ethernet de réseau local est allumé lorsqu'un des ports locaux est connecté.

      Si le voyant d'un port de réseau local est allumé, cela signifie qu'une liaison est établie avec le périphérique connecté. Si un port de réseau local est connecté à un périphérique de 100 Mbit/s, vérifiez que son voyant est allumé en vert. S'il s'agit d'un port de 10 Mbit/s, le voyant doit être orange.

   e. Le voyant de port Ethernet de réseau étendu (WAN) est allumé lorsque le routeur est connecté à un modem filaire.
   f. Le voyant de signal est allumé lorsque le routeur a détecté un signal haut débit mobile.
      - Un voyant bleu indique une excellente couverture.
      - Un voyant vert indique une bonne couverture.
      - Un voyant orange dénote une couverture partielle.

Si l'une ou l'autre de ces conditions n'est pas respectée, veuillez consulter le tableau suivant.

Voyant		Action
Alimentation 	Le voyant d'alimentation est éteint.	• Assurez-vous que le cordon d'alimentation est bien raccordé à votre routeur et que l'adaptateur secteur est correctement branché à une prise de courant fonctionnant normalement. • Assurez-vous d'utiliser l'adaptateur secteur fourni par NETGEAR avec ce produit. • Si l'erreur persiste, il se peut que le problème provienne de votre matériel. Communiquez alors avec le soutien technique.
	Le voyant d'alimentation est orange.	La défaillance se situe du côté du routeur. Essayez de corriger le problème comme suit : • Éteignez le routeur, puis rallumez-le et vérifiez qu'il s'active. • Rétablissez la configuration par défaut du routeur. L'adresse IP du routeur devient 192.168.0.1. Cette procédure est décrite dans la section *Rétablissement du mot de passe et de la configuration par défaut* à la page 192. Si l'erreur persiste, il se peut que le problème provienne de votre matériel. Communiquez alors avec le soutien technique.

Voyant		Action
Port Internet 	Le voyant Internet est éteint.	Assurez-vous que la carte SIM reçue est insérée dans le routeur. Les cartes SIM provenant d'autres appareils ne fonctionnent pas dans le routeur, et cette carte SIM ne fonctionnera pas dans d'autres appareils.
	Le voyant Internet est orange.	Le routeur ne peut pas se connecter à Internet. Vérifiez l'option de connexion Internet sélectionnée. • Pour l'option de connexion haut débit mobile, vérifiez le voyant de signal. • Pour l'option de connexion Ethernet, vérifiez le voyant de réseau étendu (WAN).
	Le voyant Internet clignote en orange et en vert.	La fonction de mesure du trafic est activée et la limite établie a été atteinte.
Liaison Wi-Fi 	Le voyant Wi-Fi est éteint.	La liaison radio Wi-Fi a été désactivée. Si vous voulez établir une connexion Wi-Fi avec le routeur, appuyez sur le bouton Wi-Fi pour réactiver la liaison radio Wi-Fi.
	Le voyant Wi-Fi ne clignote pas.	Si ce voyant ne clignote pas lorsque vous tentez de transmettre des données par liaison Wi-Fi, accédez au menu du routeur en utilisant la connexion Ethernet de réseau local et vérifiez la configuration de connexion sans fil (Wi-Fi) de votre routeur.
Ports de réseau local 	Le voyant de réseau local est éteint.	Si ce voyant ne s'allume pas lorsqu'une connexion Ethernet est établie, vérifiez les points suivants : • Assurez-vous que le câble Ethernet est correctement branché au routeur et au concentrateur ou au poste de travail. • Assurez-vous que le concentrateur ou le poste de travail connecté est sous tension.
Port WAN 	Le voyant de réseau étendu (WAN) est éteint.	Si ce voyant ne s'allume pas lorsqu'une connexion Ethernet est établie au moyen de l'option de connexion Ethernet, vérifiez les points suivants : • Assurez-vous que le câble Ethernet est correctement branché au routeur et au modem. • Assurez-vous que le modem est sous tension.
Réseau 2G/3G 	Le voyant 2G/3G est éteint.	Le routeur ne peut pas déterminer si la connexion haut débit mobile utilise des signaux 2G ou 3G.
Signal 	Le voyant de signal est éteint ou allumé en orange.	Si ce voyant ne s'allume pas lorsque la connexion haut débit mobile est utilisée, vérifiez les points suivants : • Vérifiez auprès de votre FAI si la couverture est bonne dans votre zone. • Assurez-vous que votre compte haut débit mobile est actif. • Assurez-vous que la carte SIM est correctement insérée dans le routeur. • Placez le routeur près d'une fenêtre ou à un endroit différent. Assurez-vous que le voyant de signal est allumé, ce qui vous indique qu'une couverture haut débit mobile est disponible pour le routeur. • Accédez au menu du routeur et vérifiez la configuration Internet. Vérifiez auprès du FAI si le nom d'utilisateur (identifiant), le mot de passe et le nom du point d'accès sont correctement définis. Si vous utilisez un code PIN pour établir la connexion à Internet, assurez-vous que ce code est correctement entré.

Dépannage de l'accès au menu principal du routeur

Si vous ne parvenez pas à accéder au menu principal du router à partir d'un ordinateur de votre réseau local, vérifiez les points suivants :

- Si vous utilisez un ordinateur connecté à un réseau Ethernet, vérifiez la connexion Ethernet entre l'ordinateur et le routeur en suivant la procédure décrite à la section précédente.
- Assurez-vous que l'adresse IP de votre ordinateur comporte le même sous-réseau que celui du routeur. Si vous utilisez le schéma d'adressage recommandé, l'adresse de votre ordinateur doit être comprise entre 192.168.0.2 et 192.168.0.254. Pour déterminer l'adresse IP de votre ordinateur, consultez le document en ligne proposé dans la section *Principes de base d'un réseau ITCP/IP* à l'annexe A.

Remarque : Si l'adresse IP de votre ordinateur correspond à 169.254.x.x : Les versions récentes de Windows et de Mac OS génèrent et attribuent une adresse IP lorsque l'ordinateur ne parvient pas à se connecter à un serveur DHCP. L'adresse générée automatiquement est comprise dans la plage d'adresses 169.254.x.x. Si votre adresse IP est dans cette plage, vérifiez que le routeur est bien connecté à l'ordinateur et redémarrez ce dernier.

- Si l'adresse IP du routeur a été modifiée et que vous ne connaissez pas l'adresse IP actuelle, rétablissez les paramètres par défaut du routeur. L'adresse IP du routeur devient 192.168.0.1. Cette procédure est décrite dans la section *Rétablissement du mot de passe et de la configuration par défaut* à la page 192.
- Assurez-vous que Java, JavaScript ou ActiveX sont activés dans votre navigateur. Si vous utilisez Internet Explorer, cliquez sur **Actualiser** pour vous assurer que l'applet Java est chargée.
- Essayez de fermer le navigateur puis de le rouvrir.
- Assurez-vous d'utiliser les renseignements de connexion adéquats. Le nom de connexion par défaut est **admin** et le mot de passe par défaut est **password**. Assurez-vous que le verrouillage des majuscules n'est pas activé.

Si le routeur n'enregistre pas les modifications que vous avez apportées depuis l'interface de gestion Web, vérifiez les points suivants :

- Lorsque vous modifiez les paramètres de configuration, n'oubliez pas de cliquer ensuite sur le bouton **Appliquer** avant de passer à un autre écran ou à un autre onglet, sans quoi vos modifications seront perdues.
- Cliquez sur le bouton **Actualiser** ou **Recharger** du navigateur Web. Il est possible que les modifications aient été appliquées mais que le navigateur Web affiche l'ancienne configuration stockée dans la mémoire cache.

Dépannage de la connexion au FAI

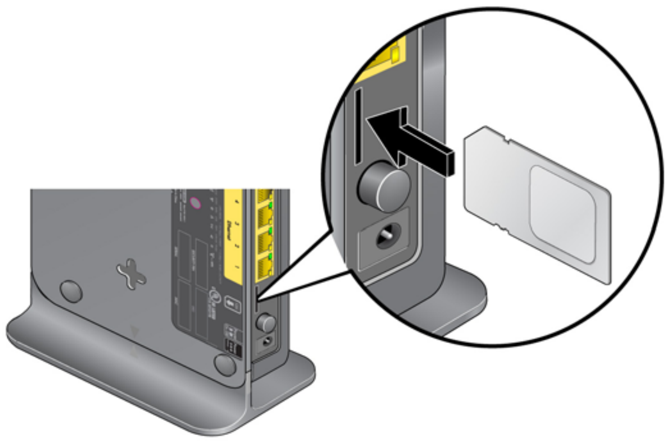
Si vous éprouvez des difficultés à vous connecter à Internet ou à naviguer sur Internet, vérifiez les causes possibles ci-dessous.

Connexion à Internet

Si vous ne parvenez pas à vous connecter à Internet, vérifiez les points suivants :

1. Le compte Internet doit être actif.

   Si votre FAI vous a remis une carte SIM et que vous ne l'avez pas encore insérée dans la fente de carte SIM à l'arrière du routeur, faites-le maintenant.

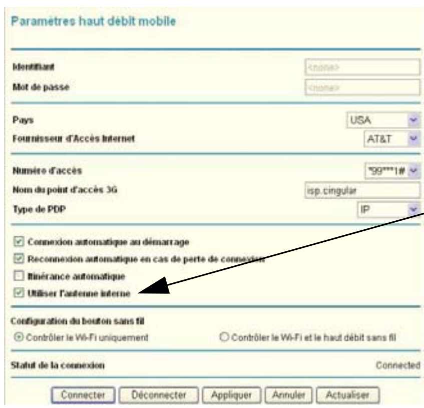


2. Une couverture haut débit sans fil doit être disponible à l'endroit où se trouve l'appareil.
3. Accédez au menu principal du routeur pour vérifier si les paramètres de connexion haut débit sont exacts. Si vous n'en êtes pas certain, informez-vous auprès de votre FAI.
4. Vérifiez l'emplacement du routeur.
   a. Rapprochez le routeur d'une fenêtre afin d'améliorer la réception du signal Internet.
      - Un voyant de signal bleu indique une excellente couverture.
      - Un voyant de signal vert indique une bonne couverture.
      - Un voyant de signal orange dénote une couverture partielle.
      - Un voyant de signal éteint indique qu'il n'y a aucune couverture.
   b. Maintenez les distances recommandées entre l'équipement NETGEAR et les appareils électroménagers afin de réduire les interférences (consultez la section *Déclaration de conformité* à la page 198).

5. Utilisation d'une antenne externe pour augmenter la puissance du signal :



a. Installez une antenne externe. (L'antenne externe est un accessoire optionnel que vous pouvez acheter.)



b. Décochez la case **Utiliser l'antenne interne** dans l'écran Paramètres haut débit mobile puis cliquez sur **Appliquer**.

c. Cliquez sur **Connecter** pour établir la connexion à Internet.

Dépannage de la navigation Internet

Si votre router obtient une adresse IP mais que votre ordinateur ne parvient pas à charger de pages Web depuis Internet :

- La mesure de trafic est activée et la limite établie a été atteinte.

  Vous pouvez rétablir l'accès Internet si vous configurez la mesure de trafic de manière à ne pas désactiver (bloquer) la connexion. Cependant, si votre compte est assorti d'une limite d'utilisation, il est possible que votre FAI vous facture des frais de dépassement de limite.

- Il se peut que votre ordinateur ne reconnaisse pas les adresses du serveur DNS.

  Un serveur DNS est un hôte Internet qui remplace les noms Internet (comme une adresse www) par des adresses IP numériques. En règle générale, votre fournisseur d'accès indique les adresses d'un ou de deux serveurs DNS que vous pouvez utiliser. Si vous avez entré une adresse DNS durant la configuration du router, redémarrez l'ordinateur et vérifiez l'adresse DNS, de la manière décrite dans l'article proposé en lien dans la section *Principes de base d'un réseau ITCP/IP* à l'annexe A. Vous pouvez également configurer manuellement votre ordinateur avec ces adresses DNS, comme expliqué dans la documentation de votre système d'exploitation.

- Il se peut que le router ne soit pas configuré dans votre ordinateur en tant que router TCP/IP.

  Si votre ordinateur obtient ses données du router par le serveur DHCP, redémarrez l'ordinateur et vérifiez l'adresse du router, de la manière décrite dans la documentation en ligne proposée dans la section *Principes de base d'un réseau ITCP/IP* à l'annexe A.

Dépannage d'un réseau TCP/IP à l’aide de l’utilitaire Ping

La plupart des routeurs et périphériques terminaux TCP/IP contiennent un utilitaire Ping qui envoie un paquet d'appel écho au périphérique désigné. Le périphérique peut alors répondre en envoyant une réponse par écho. Vous pouvez facilement résoudre les problèmes de réseau TCP/IP en vous servant de l'utilitaire Ping de votre ordinateur.

Vérification de la connexion entre le réseau local et votre routeur

Vous pouvez lancer un test Ping vers le routeur depuis votre ordinateur afin de vérifier que la connexion au réseau local est correctement configurée sur le routeur.

Pour effectuer un Ping sur le routeur à partir d’un ordinateur sous Windows95 ou une version plus récente :

1. Dans la barre d’outils Windows, cliquez sur le bouton Démarrer et choisissez Exécuter.
2. Dans le champ qui apparaît, entrez **ping** suivi de l’adresse IP du routeur, comme dans l’exemple suivant :

   ping 192.168.0.1

3. Cliquez sur **OK**.

   Un message comme celui-ci devrait apparaître :

   Envoi d'une requête Ping <adresse IP> avec 32 octets de données

   Si la connexion est établie, le message suivant apparaît :

   Réponse de <adresse IP> : octets=32 temps=NN ms TTL=xxx

   Si la connexion échoue, le message suivant apparaît :

   Request timed out (La demande a dépassé le délai imparti)

   Si la connexion n’est pas établie, cela peut être dû à l’un des problèmes suivants :

   - Mauvaises connexions physiques
     - Assurez-vous que le voyant du port de réseau local est allumé. Si le voyant est éteint, suivez les instructions de la section *Connexion à Internet* à la page 188.
     - Assurez-vous que les voyants de liaison correspondants sont allumés pour votre carte d'interface réseau et pour les ports du concentrateur qui sont connectés à votre poste de travail et au routeur (le cas échéant).
   - Mauvaise configuration réseau
     - Vérifiez que le logiciel pilote de la carte Ethernet et le logiciel TCP/IP sont bien installés et configurés sur votre ordinateur ou poste de travail.
     - Vérifiez que l’adresse IP de votre routeur et de votre poste de travail sont exactes et que celles-ci sont font partie du même sous-réseau.

Vérification de la connexion entre l'ordinateur et un périphérique distant

Après vous être assuré que la connexion entre le réseau local et le routeur est active, vérifiez la connexion entre l'ordinateur et un périphérique distant.

1. Dans la barre d'outils Windows, cliquez sur le bouton Démarrer et choisissez Exécuter.
2. Dans la fenêtre Exécuter, tapez :

   `ping -n 10` *adresse IP*

   où *adresse IP* correspond à l'adresse IP d'un périphérique distant, tel que le serveur DNS de votre fournisseur d'accès.

Si la connexion est établie, les messages mentionnés à la section précédente apparaissent. Si vous n'obtenez aucun message :

- Vérifiez que votre ordinateur et le routeur configuré comme router par défaut ont la même adresse IP. Si les paramètres IP de votre ordinateur sont configurés par DHCP, ces renseignements n'apparaîtront pas dans le panneau de configuration réseau de l'ordinateur. Vérifiez que l'adresse IP du routeur apparaît en tant que router par défaut, de la manière décrite dans la documentation en ligne proposée dans la section *Préparer votre réseau* à l'annexe A.
- Assurez-vous que l'adresse réseau de votre ordinateur (la partie de l'adresse IP spécifiée par le masque de sous-réseau) est différente de l'adresse réseau du périphérique distant.
- Assurez-vous que le modem câble ou DSL est connecté et en état de marche.
- Si votre fournisseur d'accès a attribué un nom d'hôte à votre ordinateur, entrez ce nom d'hôte en tant que nom de compte dans l'écran Basic Settings (Paramètres de base).
- Votre FAI pourrait rejeter les adresses MAC Ethernet de tous vos ordinateurs sauf un. De nombreux FAI haut débit limitent l'accès en autorisant uniquement le trafic provenant de l'adresse MAC de votre modem haut débit, mais certains FAI limitent encore davantage l'accès en autorisant l'adresse MAC d'un seul ordinateur connecté au modem. Dans ce cas, vous devez configurer votre routeur de manière à cloner ou à usurper l'adresse MAC de l'ordinateur autorisé. Consultez le *Mobile Broadband 11n Wireless Router MBR1210 Installation Guide*.

Problèmes de date et d'heure

L'écran E-mail affiche la date et l'heure actuelles. Le Mobile Broadband 11n Wireless Router utilise le protocole de synchronisation réseau NTP pour obtenir l'heure actuelle d'un des nombreux serveurs temporels réseau sur Internet. Chaque entrée de journal est estampillée avec la date et l'heure en cours. Voici quelques problèmes éventuels concernant la fonction de date et heure :

- La date affichée est le 1er janvier 2000.
  Cause : le routeur n'a pas réussi à communiquer avec un serveur temporel réseau. Assurez-vous que les paramètres d'accès Internet sont correctement configurés. Si vous venez de terminer la configuration du routeur, attendez au moins cinq minutes et revérifiez la date et l'heure.
- Il existe un décalage d'une heure.
  Cause : le routeur ne détecte pas automatiquement l'heure avancée d'été. Dans l'écran E-mail, cochez ou décochez la case **Adjust for Daylight Savings Time** (Ajustement à l'heure avancée).

Rétablissement du mot de passe et de la configuration par défaut

Cette section explique comment restaurer les paramètres de configuration par défaut, afin de rétablir le mot de passe d'administrateur **password** et l'adresse IP **192.168.0.1**. Vous pouvez effacer les paramètres de configuration actuels et rétablir les paramètres par défaut de deux manières :

- Utilisez la fonction Effacer (consultez la section *Effacement des paramètres de configuration* à la page 155).
- Appuyez pendant six secondes sur le bouton de réinitialisation situé au bas du routeur. Utilisez cette méthode lorsque vous ne connaissez pas l'adresse IP ou le mot de passe de l'administrateur.

Les paramètres par défaut sont indiqués à la section *Paramètres par défaut d'usine* à l'annexe A.

A. Information complémentaire

A

La présente annexe fournit les renseignements suivants :

- **Paramètres par défaut d'usine**
- **Caractéristiques techniques**
- **Documents connexes**

Paramètres par défaut d'usine

Appuyez sur le bouton de réinitialisation au bas du router pour rétablir tous les paramètres à leurs valeurs par défaut d'usine. Cette procédure est appelée réinitialisation à froid. Pour effectuer une réinitialisation à froid, maintenez enfoncé le bouton de réinitialisation pendant six secondes. Les paramètres du router sont rétablis à leurs valeurs par défaut d'usine (présentées dans le tableau suivant).

Fonction		Valeur par défaut
Connexion au routeur	Adresse de connexion de l'utilisateur	http://www.routerlogin.net *ou* http://www.routerlogin.com
	Nom d'utilisateur (sensible à la casse)	admin
	Mot de passe de connexion (sensible à la casse)	password
Connexion Internet	Adresse MAC (réseau étendu)	Utiliser l'adresse par défaut
	Unité de transfert maximale (MTU) de réseau étendu (WAN)	1 500
	Vitesse de port	Compatible automatique
Réseau local (LAN)	IP de réseau local	192.168.0.1
	Masque de sous-réseau	255.255.255.0
	Direction RIP	Aucun
	Version RIP	Désactivée
	Authentification RIP	Aucun
	Serveur DHCP	Activée
	Adresse IP de début DHCP	192.168.0.2
	Adresse IP de fin DHCP	192.168.0.254
	Zone démilitarisée (DMZ)	Désactivée
	Fuseau horaire	Heure de l'Est pour l'Amérique du Nord
	Ajustement à l'heure avancée	Désactivée
Pare-feu	Communications entrantes provenant d'Internet	Désactivées (sauf sur le port 80, le port HTTP)
	Communications sortantes en direction d'Internet	Activées (toutes)
	Filtrage MAC source	Désactivée

Fonction (suite)		Valeur par défaut (suite)
Modem haut débit mobile	Fournisseur d'accès Internet	Bell Mobilité
	Nom du point d'accès	inet.bell.ca
	Numéro d'accès	*99#
	Type de PDP	IP
	Nom d'utilisateur	Aucun requis
WiFi	Communication sans fil	Activée
	Nom de réseau sans fil (SSID)	See label on the bottom of router
	Sécurité	WPA-PSK/WPA2-PSK mode mixte
	Diffusion du nom de réseau sans fil	Activée
	Vitesse de transmission	Automatique (vitesse maximale du signal sans fil conformément à la norme IEEE 802.11. Le débit réel peut varier. L'état du réseau et les conditions d'utilisation, notamment le volume du trafic, les matériaux et la structure du bâtiment ainsi que le surdébit du réseau, diminuent la vitesse de transmission des données.)
	Pays/région	Canada
	Canal radio	Automatique
	Mode de fonctionnement	Jusqu'à 145 Mbits/s
	Débit de transfert de données	Meilleur
	Puissance de sortie	Maximale
	Point d'accès	Activée
	Type d'authentification	Système ouvert
	Liste d'accès de cartes sans fil	Toutes les stations sans fil permises

Caractéristiques techniques

Caractéristiques techniques	
Protocole réseau et normes	TCP/IP, DHCP
Un adaptateur secteur	• Amérique du Nord : 120V CA, 60 Hz, entrée • 12 V CC A 1,5 A sortie
Caractéristiques physiques	• Dimensions : 6,8 po x 5,03 po x 1,28 po (173 mm x 128 mm x 33 mm) • Poids : 0,65 lb sans le support (0,29 kg)
Spécifications environnementales	• Températures de fonctionnement : de 0°C à 40°C (de 32ºF à 104ºF) • Humidité de fonctionnement : humidité relative de 90 % maximum, hors condensation
Émissions électromagnétiques	Article 15 de la FCC, classe B; IC, EN 55 022 (CISPR 22), classe B
Caractéristiques d’interface	• Réseau local (LAN) : 10BASE-T ou 100BASE-Tx, RJ-45 • WAN : 10BASE-T ou 100BASE-Tx, RJ-45
Connexion de l'antenne (facultative)	• Connecteur R-TNC

Documents connexes

Le tableau ci-dessous contient des liens vers des documents de référence qui peuvent vous aider à mieux comprendre les technologies utilisées par votre produit NETGEAR.

Document	Lien
Utilisation de Microsoft Windows Vista ou Windows XP pour gérer les connexions réseau sans fil	*http://documentation.netgear.com/reference/enu/winzerocfg/index.htm*
Principes de base d'un réseau ITCP/IP Principes de base d'un réseau sans fil	*http://documentation.netgear.com/reference/enu/tcpip/index.htm* *http://documentation.netgear.com/reference/enu/wireless/index.htm*
Préparer votre réseau	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Principes de base d'un réseau privé virtuel	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossaire	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

Avis de conformité

B

Routeurs sans fil, passerelles et points d'accès NETGEAR

Déclaration de conformité

Cette section décrit les exigences que doit respecter l'utilisateur concernant l'utilisation de ce produit conformément aux lois et règlements nationaux en matière d'utilisation du spectre des radiofréquences et des appareils radio. Le non-respect par l'utilisateur final des exigences applicables peut entraîner un fonctionnement illégal et une action en justice contre l'utilisateur final par les autorités réglementaires nationales.

Remarque : Le fonctionnement du micrologiciel de ce produit est limité aux canaux permis dans une région ou un pays donné. Par conséquent, certaines options décrites dans le présent guide pourraient ne pas être disponibles dans votre version du produit.

Exigences de la FCC concernant l'utilisation du produit aux États-Unis

Information de la FCC destinée à l'utilisateur

Ce produit ne contient aucune pièce pouvant être réparée par l'utilisateur et il doit être utilisé uniquement avec les antennes approuvées. Tout changement ou modification du produit annulera l'ensemble des certifications et approbations réglementaires applicables.

Directives de la FCC concernant l'exposition des personnes

Cet appareil est conforme aux limites d'exposition aux rayonnements de la FCC pour un environnement non contrôlé. Il doit être installé de façon à garder une distance minimale de 20 centimètres entre la source de rayonnements et votre corps.

L'émetteur ne doit pas être colocalisé ni fonctionner conjointement avec une autre antenne ou un autre émetteur.

Déclaration de conformité à la FCC

Nous, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, déclarons sous notre responsabilité exclusive que le Routeur sans fil MBR1210 11n à haut débit mobile est conforme à la Section 15, Sous-section B, des règlements FCC CFR47. Son fonctionnement est sujet aux deux conditions suivantes :

- Cet appareil ne doit pas provoquer d'interférences nuisibles; et
- Cet appareil doit accepter toutes les interférences reçues, y compris celles pouvant causer un fonctionnement indésirable.

Avertissements et directives en matière de brouillage radioélectrique de la FCC

Cet appareil a été testé et certifié conforme aux restrictions pour les appareils numériques de Classe B, conformément à l'article 15 de la réglementation de la FCC. Ces restrictions visent à garantir une protection suffisante contre les interférences nuisibles dans une installation à domicile. Cet appareil utilise et peut diffuser des fréquences radio. S'il n'est pas installé et utilisé conformément aux instructions, il peut provoquer des interférences nuisibles aux communications radio. Cependant, il se peut que des interférences se produisent dans une installation particulière. Pour déterminer si cet appareil produit des interférences nuisibles à la réception de la radio ou de la télévision, éteignez puis rallumez l'appareil. Si c'est le cas, nous vous recommandons de suivre les instructions ci-dessous pour éliminer les interférences :

- Réorientez l'antenne de réception.
- Éloignez davantage l'appareil du récepteur.

- Branchez l’appareil sur un circuit électrique différent de celui où le récepteur radio est branché.
- Consultez le vendeur ou un technicien expérimenté pour obtenir de l’aide.

Mise en garde de la FCC

- Les changements ou modifications non expressément approuvées par les autorités compétentes en matière de conformité peuvent priver l’utilisateur du droit d’utiliser l’équipement en question.
- Cet appareil est conforme aux limites imposées par la Section 15 de la réglementation FCC. Son fonctionnement est soumis aux deux conditions suivantes : (1) ce périphérique ne doit pas provoquer d’interférences nuisibles; et (2) ce périphérique doit accepter les interférences reçues, y compris celles qui peuvent entraîner un fonctionnement non souhaité.
- Pour les produits commercialisés aux États-Unis, seul le canal 1~11 peut être utilisé. La sélection d'autres canaux n'est pas possible.
- Cet appareil et son antenne (ou ses antennes) ne doivent pas être colocalisés ni fonctionner conjointement avec une autre antenne ou un autre émetteur.

Règlement sur le brouillage radioélectrique du ministère des Communications du Canada

Cet appareil numérique (Routeur sans fil MBR1210 11n à haut débit mobile) ne dépasse pas les limitations de la classe B en matière de transmission de bruit radioélectrique des appareils numériques, qui sont établies dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

Europe – Déclaration de conformité pour l'UE

Le symbole ci-dessus indique que l'appareil est conforme aux exigences essentielles de la directive Équipements radio et équipements terminaux de télécommunication (R&TTE) de l'Union européenne (1999/5/EC).

Cet appareil respecte les normes de conformité suivantes :

- EN300 328 (2,4 GHz), EN301 489-17, EN301 893 (5 GHz), EN60950-1
- Cet appareil est un système de transmission haut débit à 2,4 GHz (émetteur-récepteur), conçu pour être utilisé dans tous les pays membres de l'UE et de l'AELE, sauf en France et en Italie où des restrictions particulières s'appliquent.
- En Italie, l'utilisateur final doit présenter une demande de licence aux autorités nationales régissant le spectre des radiofréquences, afin d'obtenir l'autorisation d'instaurer des liaisons radio à l'extérieur ou de fournir un accès public à des services de télécommunications ou des services réseau.
- Cet appareil ne peut pas être utilisé pour instaurer des liaisons radio à l'extérieur en France et, dans certaines régions, la puissance de sortie haute fréquence peut être limitée à 10 MW PIRE dans la bande de fréquences de 2454 à 2483,5 MHz. Pour obtenir des renseignements détaillés, communiquez avec les autorités nationales régissant le spectre des radiofréquences en France.

Pour consulter la déclaration de conformité complète, rendez-vous sur le site Web des déclarations de conformité pour l’UE de NETGEAR à l’adresse : *http://kb.netgear.com/app/answers/detail/a_id/11621/*

Tableau 1. Déclaration de conformité dans les langues de la Communauté européenne

Langue	Déclaration
Cesky [tchèque]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [danois]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [allemand]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.

Tableau 1. Déclaration de conformité dans les langues de la Communauté européenne

Langue	Déclaration
Eesti [estonien]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Anglais	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [espagnol]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [grec]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français	Par la présente, *NETGEAR Inc.* déclare que cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [italien]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [letton]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [lituanien]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [néerlandais]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [maltais]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [hongrois]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [polonais]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [portugais]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [slovène]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.

Tableau 1. Déclaration de conformité dans les langues de la Communauté européenne

Langue	Déclaration
Slovensky [slovaque]	*NETGEAR Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [finnois]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [suédois]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Íslenska [islandais]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [norvégien]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

Tableau de réduction du brouillage

Le tableau ci-dessous montre la distance minimale recommandée entre l'appareil NETGEAR et les appareils électroménagers afin de réduire les interférences (indiquée en mètres et en pieds).

Tableau 2. Tableau de réduction du brouillage

Appareil électroménager	Distance minimale recommandée (en mètres et en pieds)
Fours à micro-ondes	9 mètres / 30 pieds
Interphones de surveillance – analogiques	6 mètres / 20 pieds
Interphones de surveillance – numériques	12 mètres / 40 pieds
Téléphone sans fil – analogiques	6 mètres / 20 pieds
Téléphone sans fil – numériques	9 mètres / 30 pieds
Appareils Bluetooth	6 mètres / 20 pieds
Appareils ZigBee	6 mètres / 20 pieds

Index

N

O

P

Q

R

S

U

V

W